ForeRunner® ES-3810 Configuration Manual

MANU0220-02 - Rev. A - July, 1998

Software Versions 4.13.x and 5.1.x

FORE Systems, Inc.

1000 FORE Drive
Warrendale, PA 15086-7502
Phone: 724-742-4444
FAX: 724-742-7742

http://www.fore.com

Legal Notices

TRADEMARKS

FCC CLASS A NOTICE

WARNING: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void this user's authority to operate this equipment.

NOTE: The ASX-200WG, the ASX-200BX, the ASX-1000, and the *ForeRunnerLE*™ 155 have been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of the equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

DOC CLASS A NOTICE

This digital apparatus does not exceed Class A limits for radio noise emission for a digital device as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

VCCI CLASS 1 NOTICE

この装置は、第一種情報処理装置（商工業地域において使用されるべき情報処理装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会(VCCI)基準に適合しております。
従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。
取扱説明書に従って正しい取り扱いをして下さい。

This equipment is in the Class 1 category (Information Technology Equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council For Interference by Information Technology Equipment aimed at preventing radio interference in commercial and/or industrial areas.Consequently, when used in a residential area or in an adjacent area thereto, radio interference may be caused to radios and TV receivers, etc. Read the instructions for correct handling.

FCC REQUIREMENTS (Notice to Users of DS1 Service)

The following instructions are provided to ensure compliance with the FCC Rules, Part 68.

(1) This device must only be connected to the DS1 network connected behind an FCC Part 68 registered channel service unit. Direct connection is not allowed.

(2) Before connecting your unit, you must inform the telephone company of the following information:

Port ID	REN/SOC	FIC	USOC
NM-6/DS1C	6.0N	04DU9-BN, 04DU9-DN,	RJ48C
NM-2/DS1C	6.0N	04DU9-1ZN, and 04DU9-1SN	RJ48C

(3) If the unit appears to be malfunctioning, it should be disconnected from the telephone lines until you learn if your equipment or the telephone line is the source of the trouble. If your equipment needs repair, it should not be reconnected until it is repaired.

(4) If the telephone company finds that this equipment is exceeding tolerable parameters, the telephone company can temporarily disconnect service, although they will attempt to give you advance notice if possible.

(5) Under the FCC Rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or out of warranty.

(6) If the telephone company alters their equipment in a manner that will affect use of this device, they must give you advance warning so as to give you the opportunity for uninterrupted service. You will be advised of your right to file a complaint with the FCC.

CANADIAN IC CS-03 COMPLIANCE STATEMENT

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Industry Canada label does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

E1 AND E3 NOTICE

The E1 (NM-6/E1C and NM-2/E1C) and E3 (NM-4/E3C and NM-2/E3C) network modules that are described in this manual are approved for use in FORE Systems' host systems providing that the instructions below are strictly observed. Failure to follow these instructions invalidates the approval.

Pan European Approval - CE Marking

Pan European approval of the E1 network module was issued by BABT following assessment against CTR12. This means that it can be connected to ONP and unstructured PTO-provided private circuits with 120 Ω interfaces in all European countries, according to Telecommunications Terminal Equipment (TTE) Directive 91/263/EEC. Thus, the following CE mark applies:

CE168X

The E1 and E3 network modules conform to safety standard EN60950 1992 following the provisions of Low Voltage Product Safety Directive 73/23/EEC and CE Marking Directive 93/68/EEC, and can be marked accordingly with the CE symbol.

The E1 and E3 network modules conform to EN55022 1994 and EN50082-1 1992 following the provisions of the EMC Directive 89/336/EEC, and can be marked accordingly with the CE symbol.

National Approvals

UK

Network Module	Connects to	Approval Number
E1	Structured and unstructured PTO-provided private circuits with 75 Ω interfaces	AA60953
E3	PTO-provided private circuits with 75 Ω interfaces	NS/4387/1/T/605954

Germany

Network Module	Connects to	Approval Number
E3	Structured PTO-provided private circuits with 75 Ω interfaces	A127535H for the ASX-1000 A127534H for the ASX-200BX or ASX-200WG

Switzerland

Network Module	Connects to	Approval Number
E1	Structured PTO-provided private circuits with 120 Ω interfaces	96.0872.J.N
E3	Structured PTO-provided private circuits with 75 Ω interfaces	96.0873.J.N

Required User Guide Statements - UK Installation

The use of auxiliary products not authorized by FORE Systems® in FORE Systems ATM Switches may cause the power specification to be exceeded and is a potential safety hazard.

The equipment must be installed such that with the exception of the connections to the host, clearance and creepage distances shown in the table below are maintained between the network module and any other assemblies which use or generate a voltage shown in the table below. The larger distance shown in brackets applies where the local environment within the host is subject to conductive pollution or dry non-conductive pollution which could become conductive due to condensation. Failure to maintain these minimum distances invalidates the approval.

Clearance (mm)	Creepage (mm)	Voltage Used or Generated by Host or by Network Modules
2.0	2.4 (3.8)	Up to 50 V_{rms} or V_{dc}
2.6	3.0 (4.8)	Up to 125 V_{rms} or V_{dc}
4.0	5.0 (8.0)	Up to 250 V_{rms} or V_{dc}
4.6	6.4 (10.0)	Up to 300 V_{rms} or V_{dc}

For a host or other expansion card fitted in the host, using or generating voltages greater than 300V (rms or dc), advice from a competent telecommunications engineer must be obtained before installation of the relevant equipment.	Above 300 V_{rms} or V_{dc}

NOTE: Installing the network modules in the appropriate FORE Systems hosts, according to the installation instructions provided, satisfies the requirements listed above.

The following tables show the available ports and their safety status:

NM-6/E1C and NM-2/E1C

Ports	Safety Status
E1 Ports	TNV operating at SELV
Bus Connector	SELV

NM-4/E3C and NM-2/E3C

Ports	Safety Status
E3 Ports	TNV operating at SELV
Bus Connector	SELV

CE NOTICE

Marking by the symbol **CE** indicates compliance of this system to the EMC (Electromagnetic Compatibility) directive of the European Community and compliance to the Low Voltage (Safety) Directive. Such marking is indicative that this system meets or exceeds the following technical standards:

- EN 55022 - "Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment."
- EN 50082-1 - "Electromagnetic compatibility - Generic immunity standard Part 1: Residential, commercial, and light industry."
- IEC 1000-4-2 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 2: Electrostatic discharge requirements."
- IEC 1000-4-3 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 3: Radiate electromagnetic field requirements."
- IEC 1000-4-4 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 4: Electrical fast transient/burst requirements."

SAFETY CERTIFICATIONS

ETL certified to meet Information Technology Equipment safety standards UL 1950, CSA 22.2 No. 950, and EN 60950.

ALPHA/BETA TEST DISCLAIMER

This ALPHA/BETA equipment has not been tested and found to comply with the emissions limits. These limits are designed to provide reasonable protection against harmful interference. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference with radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: 1) Reorient or relocate the receiving antenna. 2) Increase the separation between the equipment and the receiver. 3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. 4) Consult FORE Systems, Inc. for more help. This equipment is to be used for evaluation purposes. Changes must not be made without the prior proper approval of FORE Systems, Inc.

This device has not been approved by the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased until the approval of the FCC has been obtained.

Table of Contents

APPENDIX A ESM-16 Console Management Subsystem

Preface

This manual provides users of the *ForeRunner*® ES-3810 Ethernet Workgroup Switch with the information to configure and manage the ES-3810. For additional configuration information, refer to the *ForeRunner*® *Basic Configuration Manual.* If you have questions or problems with the installation, please contact FORE Systems Technical Assistance Center (TAC). (See "Technical Support" on page ii..)

Chapter Summaries

Chapter 1 - Introduction - Provides information about the Network Management Module, the ES-3810's console interface, and logon procedures.

Chapter 2 - System Management - Provides information about viewing and configuring ES-3810 system parameters, viewing installed modules, and managing system software.

Chapter 3 - Interface Management - Provides information about the management and configuration of the ES-3810's Ethernet and ATM interfaces, describes LANE and RFC 1483 (PVC) configuration, and describes the ES-3810's various interface counters.

Chapter 4 - VLAN Management - Describes how to create, modify, and delete VLANs, including naming, port and MAC address inclusion, IGMP filtering, and protocol (LANE or RFC1483) usage.

Chapter 5 - UDP/IP Management - Describes management of the ARP cache, IP parameters, and the IP routing table, as well as how to view ICMP, IP, and UDP counters.

Chapter 6 - SNMP Management - Describes how to modify and manage the Access Control List and the Trap Destination List, and how to view SNMP counters.

Chapter 7 - Spanning Tree Management - Describes how to create, modify, and delete Spanning Tree instances on the ES-3810, how to display the Spanning Tree configuration, and how to configure Spanning Tree on individual ports.

Chapter 8 - Telnet Management - Describes how to view the current Telnet parameters, how to enable or disable Telnet on the ES-3810, and how to modify the timeout value on the switch.

Chapter 9 - MPOA Management - Describes how to view the current MPOA parameters and MPC counters, how to manage MPC, and how to control ATM addresses.

Appendix A - ESM-16 Console Management Subsystem - Provides information about local management of the ES-3810 via the ESM-16.

Technical Support

In the U.S.A., customers can reach FORE Systems' Technical Assistance Center (TAC) using any one of the following methods:

1. Select the "Support" link from FORE's World Wide Web page:

   http://www.fore.com/

2. Send questions, via e-mail, to:

   support@fore.com

3. Telephone questions to "support" at:

   800-671-FORE (3673) or **724-742-6999**

4. FAX questions to "support" at:

   724-742-7900

Technical support for customers outside the United States should be handled through the local distributor or via telephone at the following number:

+1 724-742-6999

No matter which method is used to reach FORE Support, customers should be ready to provide the following:

- A support contract ID number
- The serial number of each product in question
- All relevant information describing the problem or question

Typographical Styles

Throughout this manual, specific commands to be entered by the user appear on a separate line in bold typeface. In addition, use of the `Enter,` or `Return,` key is represented as `<ENTER>`. The following example demonstrates this convention:

`cd \usr` `<ENTER>`

Commands, menu options, or file names that appear within the text of this manual are represented in the following style: "...the `fore_install` program will install this distribution"

Important Information Indicators

To call your attention to safety and otherwise important information that must be reviewed to insure correct and complete installation, as well as to avoid damage your system, FORE Systems utilizes the following *WARNING/CAUTION/NOTE* indicators.

WARNING statements contain information that is critical to the safety of the operator and/or the system. Do not proceed beyond a ***WARNING*** statement until the indicated conditions are fully understood or met. This information could prevent serious damage to the operator, the system, or currently loaded software. For example:

WARNING!

Hazardous voltages are present. To lessen the risk of electrical shock and danger to personal health, follow the instructions carefully.

CAUTION statements contain information that is important for proper installation/operation. ***CAUTION*** statements can prevent possible equipment damage or loss of data. For example:

CAUTION

You risk damaging your equipment and/or software if you do not follow these instructions.

NOTE statements contain information that has been found important enough to be called to the special attention of the operator. For example:

Steps 1, 3, and 5 are similar to the installation for the computer type above. Review the previous installation procedure before installation in your particular model.

Laser Notice

Class 1 Laser Product:
This product conforms to applicable requirements of 21 CFR 1040 at the date of manufacture.

Class 1 lasers are defined as products which do not permit human access to laser radiation in excess of the accessible limits of Class 1 for applicable wavelengths and durations. These lasers are safe under reasonably foreseeable conditions of operation. Do not view beam with optical instruments.

Every ES-3810 module with a single mode fiber optic interface contains a Class 1 laser.

Safety Precautions

For your protection, observe the following safety precautions when setting up your equipment:

- Follow all warnings and instructions marked on the equipment.
- Ensure that the voltage and frequency of your power source matches the voltage and frequency inscribed on the equipment's electrical rating label.
- Never push objects of any kind through openings in the equipment. Dangerous voltages may be present. Conductive foreign objects could produce a short circuit that could cause fire, electric shock, or damage to your equipment.

Modifications to Equipment

Do not make mechanical or electrical modifications to the equipment. FORE Systems, Inc. is not responsible for regulatory compliance of a modified FORE product.

Placement of a FORE Systems Product

CAUTION

To ensure reliable operation of your FORE Systems product and to protect it from overheating, openings in the equipment must not be blocked or covered. A FORE Systems product should never be placed near a radiator or heat register.

Power Cord Connection

WARNING!

FORE Systems AC-powered products are designed to work with single-phase power systems having a grounded neutral conductor. To reduce the risk of electrical shock, do not plug FORE Systems products into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.

WARNING!

Your AC-powered FORE Systems product is shipped with a grounding type (3-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.

CHAPTER 1 Introduction

The system and network management capabilities of the ES-3810 are provided by the Network Management Module (NMM) and the Network Management Controller (NMC). The primary functions of the NMM / NMC are as follows:

- Provide SNMP-based management for the ES-3810 Ethernet Workgroup switch
- Provide a management console that permits the configuration of both system-wide (e.g., IP Address, Subnet Mask) and port-specific (e.g., Sniffing Mode, Backbone Mode) parameters

The NMM / NMC is the management vehicle for the ES-3810, whether installed with or without the ESM-16 management module. In cases where both modules are installed in a switch, the NMM / NMC disables the management processor of the ESM-16 while allowing the 16 ports of the ESM-16 to remain active.

Some of the main functions the local management console allows the Network Administrator to perform are as follows:

- View network activity on a per port basis
- View the configuration of a particular port
- Configure each port with unique characteristics, if necessary
- Update the ES-3810's firmware
- View / modify a port's address database entries
- Save the ES-3810's unique port settings in non-volatile storage
- Reset the ES-3810

The management console utilizes a VT-100 terminal or VT-100 terminal emulator as an interface to the end-user. The system does not allow an escape from the menus— all options must be performed from a menu selection.

NOTE

The menu system operates as an autonomous subsystem of the ES-3810. If a management station is not connected to the console port, the ES-3810 still operates using either the factory default settings detailed in the *ForeRunner ES-3810 Installation and Maintenance Manual* or the last saved settings which are restored during the power up sequence.

1.1 The User Interface

The user interface to the ES-3810 is displayed on the management station (if attached) as soon as the NMM / NMC completes its internal power-up diagnostics. It is recommended that a console always be connected when the NMM / NMC is turned on so that any power-up errors may be detected (see the *ForeRunner ES-3810 Installation and Maintenance Manual*).

The management console uses the VT-100 line drawing set. If your terminal (or terminal emulation package) does not support this feature, some console text may appear twice.

1.1.1 Counter Updates

Certain screens in the ES-3810 console interface provide the ability to adjust how often the displayed data is updated. On counters and displays where automatic updates are supported, the following commands are available:

- **+** Increases the frequency with which the screen is updated to a maximum of every two seconds.
- **-** Decreases the frequency with which the screen is updated. There is no minimum update value.
- **f** Freezes the screen as it appears (i.e., the screen will not be updated).
- **u** Unfreezes the screen (i.e., the screen will be updated at the next regular interval).
- **q** Exits the screen.

1.1.2 Logging on to the ES-3810

Upon the first successful power-up of the ES-3810, you will be prompted for a username. Enter one of the following usernames according to the access privileges you want:

public Grants read only privileges to objects that are accessible through the ES-3810's local management console (e.g., port counters can be viewed, but port parameters can not be changed).

private Grants read / write privileges to all managed objects that are accessible through the ES-3810's local management console.

Logging on as `private` requires the use of a password. The default password is `fore`.

Usernames and passwords can be changed from the ES-3810 console. See Chapter 6 for more information.

Only users with read-write access can change usernames and passwords.

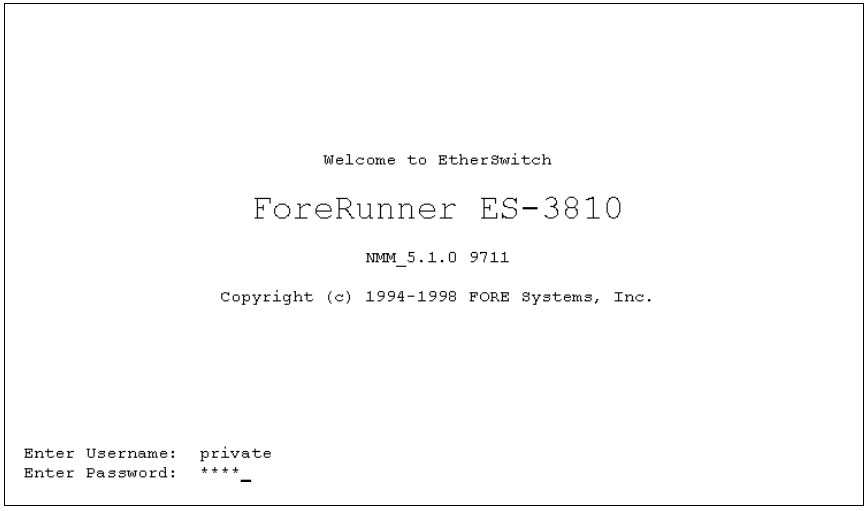


Figure 1.1 - ES-3810 Logon Screen

Once you have gained access to the ES-3810, you can modify, add, or delete usernames and the read / write privileges associated with them.

The following ES-3810 Main Menu appears once you have entered a valid username:

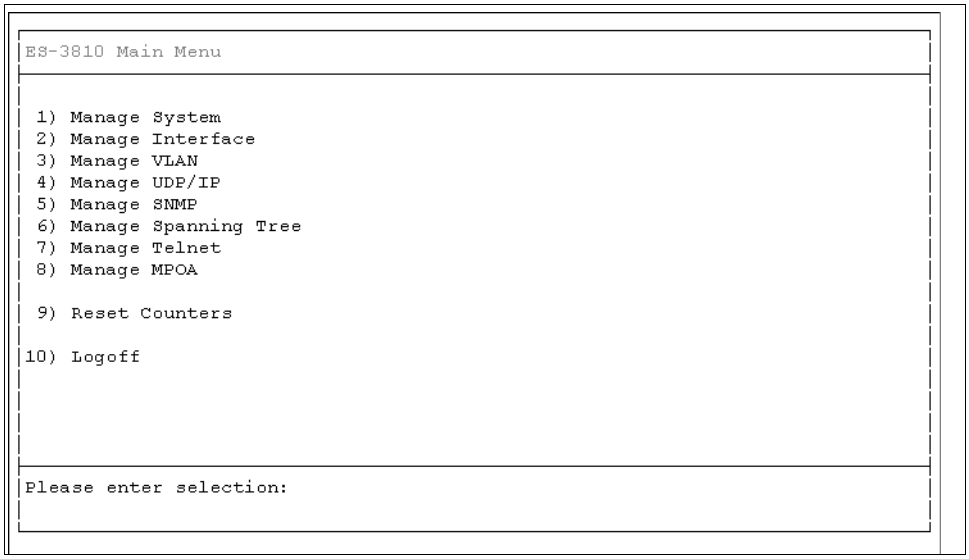


Figure 1.2 - ES-3810 Main Menu

The items in the previous menu have the following meanings:

Manage System Displays the Manage System Menu (Chapter 2).

Manage Interface Displays the Interface Selection screen (Chapter 3).

NOTE Once the user provides an interface selection, the management console displays the Manage Interface Menu, which is specific to the type of interface selected. For information on specific modules, see Chapter 3.

Manage VLAN	Displays the Manage VLAN Menu (Chapter 4).
Manage UDP/IP	Displays the Manage UDP / IP Menu (Chapter 5).
Manage SNMP	Displays the Manage SNMP Menu (Chapter 6).
Manage Spanning Tree	Displays the Manage Spanning Tree Menu (Chapter 7).
Manage Telnet	Displays the Manage Telnet Menu (Chapter 8).
Manage MPOA	Displays the Manage MPOA Menu (Chapter 9).
Reset Counters	Resets all counters in the entire system to 0. The SNMP sysUpTime value is also reset to 0.
Logoff	Returns to the logon screen.

1.1.3 Resetting Counters

To reset the counters (e.g., IP Counters, ICMP Counters, SNMP Counters, etc.) on the ES-3810, type 9 and press <ENTER> at the Main Menu. You will be prompted to confirm your choice. To reset the counters, type **y** and press <ENTER>, to abort the command, type **n** and press <ENTER>, or simply press <ENTER> (see Figure 1.3).

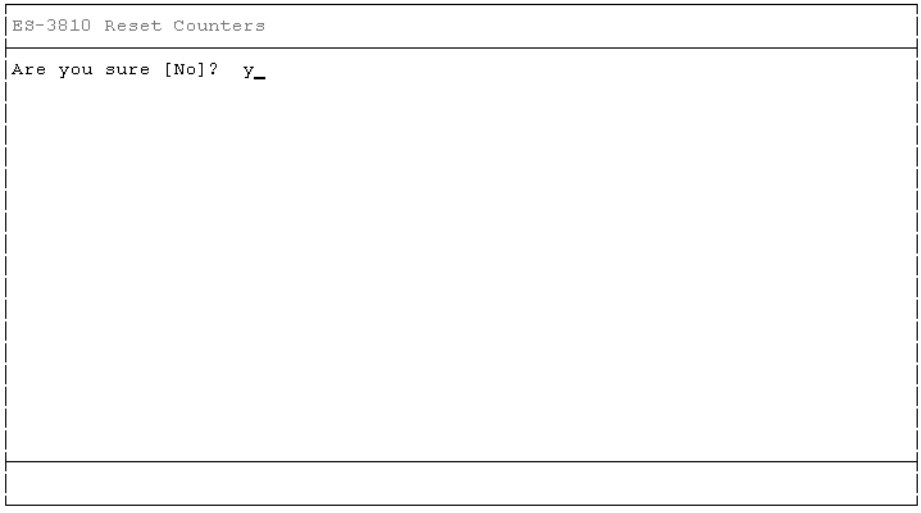


Figure 1.3 - Reset Counters Screen

1.1.4 Logging off of the ES-3810

To end a console session on the ES-3810, type **10** and press <ENTER> at the Main Menu. Logging off returns the console to the logon screen (see Figure 1.1).

CHAPTER 2 System Management

2.1 Manage System Menu

The Manage System Menu contains options that provide access to managed objects having system-wide implications. This menu is reached from the Manage System option on the Main Menu. Figure 2.1 illustrates the Manage System Menu.

```
ES-3810 Manage System Menu

 1) Return to Main Menu

 2) Manage System Parameters
 3) Manage Module
 4) Manage Software

 5) Save Current Configuration
 6) Restore Factory Default Configuration
 7) Restore Last Saved Configuration
 8) Upload Current Configuration to TFTP Server
 9) Download Configuration from TFTP Server

10) Reboot System




Please enter selection:
```

Figure 2.1 - Manage System Menu

The items in the previous menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Manage System Parameters	Displays the Manage System Parameters Menu.
Manage Module	Displays the Module Selection screen.
Manage Software	Displays the Software Selection screen.

Save Current Configuration	Saves the value of each managed object in the current configuration to persistent storage. However, some dynamic values (i.e., address database entries) will not be saved.
Restore Factory Default Configuration	Restores the value of each managed object in the current configuration to its factory default setting.
Restore Last Saved Configuration	Restores the value of each managed object in the current configuration to the value last saved to persistent storage.
Reboot System	Performs a cold restart of the system.

2.1.1 Manage System Parameters Menu

This menu displays commands that provide access to various system-wide interface parameters, it is accessed by selecting option 1 at the Manage System Menu. Figure 2.2 illustrates the Manage System Parameters Menu.

```
ES-3810 Manage System Parameters Menu

 1) Return to Main Menu
 2) Return to Previous Menu

 3) View System Parameters

 4) Modify System Name
 5) Modify System Contact
 6) Modify System Location

 7) Modify Maximum Address Database Age
 8) Modify Initial Filtering Mode

Please enter selection:
```

Figure 2.2 - Manage System Parameters Menu

The items in the previous menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage System Menu.
View System Parameters	Displays the System Parameters View screen.
Modify System Name	Queries the user for a new system name. The new system name defaults to the current system name if the user provides no input.
Modify System Contact	Queries the user for a new system contact. The new system name defaults to the current system contact if the user provides no input.
Modify System Location	Queries the user for a new system location. The new system location defaults to the current system location if the user provides no input.
Modify Maximum Address Database Age	Queries the user for a new maximum address database age value. The new maximum address database age defaults to the current maximum address database age if the user provides no input. To disable aging, enter **0** at the prompt.
Modify Initial Filtering Mode	Queries the user for a new initial filtering mode. The choices are “positive” and “negative.”

2.1.1.1 View System Parameters

This view is reached through the Manage System Menu, then through the Manage System Parameters Menu. Figure 2.3 illustrates the System Parameters View screen.

```
ES-3810 View System Parameters

System Name:          ForeRunner ES-3810
System Contact:       Contact Name
System Location:      Warrendale, PA

MAC Address:          00-A0-36-00-93-E5
System Up Time:       12:10
Kernel Up Time:       13:12.16
Memory Installed:     8388608

Maximum Address Database Age:  Aging Disabled
Initial Filtering Mode:        positive

Hit <Enter> to continue.
```

Figure 2.3 - System Parameters View

2.1.2 Manage Module Menu

This menu displays commands that monitor and control the previously selected module. This menu is reached from the Main Menu through the Manage System Menu, then through the Manage Module option. After a module is selected in the Module Selection screen, this menu will appear with options for the management of the selected module. Figure 2.4 depicts the Manage Module Menu.

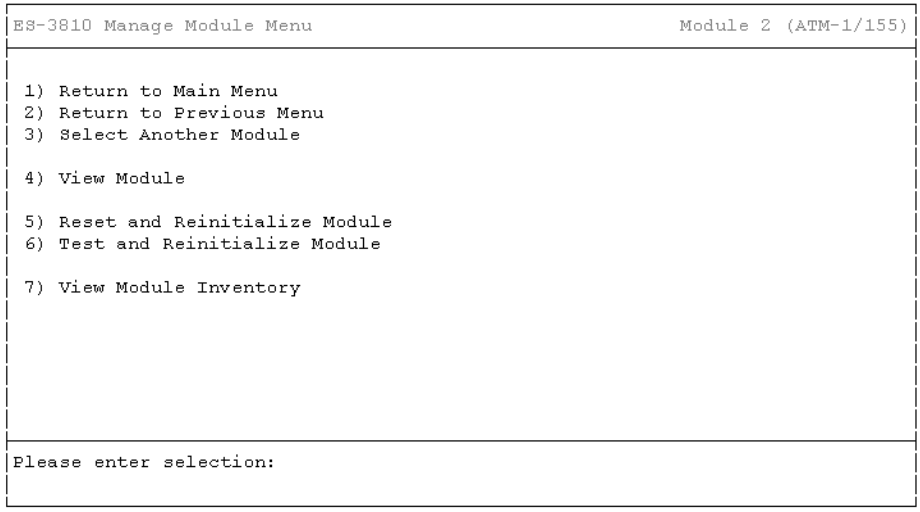


Figure 2.4 - Manage Module Menu

The options in the Manage Module Menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage System Menu.
Select Another Module	Returns to the Module Selection screen.
View Module	Displays the Module View screen for the selected module.
Reset Module	Resets the selected module.

Test Module Performs an on-line diagnostic on the selected module. When the diagnostic has completed, the selected module is reset to the last saved configuration, and the management console displays the Module Test View screen.

View Module Inventory Displays the Module Inventory View screen.

NOTE The Module View and Module Test View screens vary depending on the selected module. For information on specific modules, see Chapter 3.

2.1.2.1 Module Selection Menu

This menu asks the user to select a module from those installed on the system. This screen is reached from the Main Menu through the Manage System Menu. Figure 2.5 illustrates the Module Selection screen.

NOTE The management console does not allow the user to select an empty slot.

```
ES-3810 Module Selection

Slot | Type      | State    | Description
-----+-----------+----------+-------------------------------------------
  1  | FEM-2/TX  | Enabled  | 2-port 100BaseTX Ethernet Switch Module
  2  | ATM-1/155 | Enabled  | OC-3/155MM ATM Backbone Interface Module
  3  | SSM-16/TX | Enabled  | 16 Port-10BaseTX Segment Switch Module
  4  | ESM-24    | Enabled  | 24-port 10BaseT Ethernet Switch Module
  5  | NMM       | Enabled  | Network Management Module
  6  | ATM-1/155 | Enabled  | OC-3/155MM ATM Backbone Interface Module
  7  | PS-AC     | Enabled  | AC 110-220V Powersupply
  8  | PS-AC     | Enabled  | AC 110-220V Powersupply
                             25H
Please enter selection (by Slot):  _
```

Figure 2.5 - Module Selection Menu

After a valid module is entered, the Manage Module Menu is displayed.

2.1.2.2 Module Inventory View

This view is reached from the Main Menu through the Manage System Menu, then through the Manage Module Menu screen, and finally through the Module Selection, after a module has been selected (see Section 2.1.2.1 and Figure 2.5). Figure 2.6 illustrates the Module Inventory View screen.

ES-3810 Module Selection — Module 2 (ATM-1/155)

Slot	Type	State	Description
1	FEM-2/TX	Enabled	2-port 100BaseTX Ethernet Switch Module
2	ATM-1/155	Enabled	OC-3/155MM ATM Backbone Interface Module
3	SSM-16/TX	Enabled	16 Port-10BaseTX Segment Switch Module
4	ESM-24	Enabled	24-port 10BaseT Ethernet Switch Module
5	NMM	Enabled	Network Management Module
6	ATM-1/155	Enabled	OC-3/155MM ATM Backbone Interface Module
7	PS-AC	Enabled	AC 110-220V Powersupply
8	PS-AC	Enabled	AC 110-220V Powersupply

Please enter selection (by Slot):

Figure 2.6 - Module Inventory View

2.1.3 Manage Software Menu

This menu displays commands that monitor and control the software installed in the system. This menu is reached from the Main Menu through the Manage System Menu, then through the Manage Software option. Figure 2.7 illustrates the Manage Software Menu.

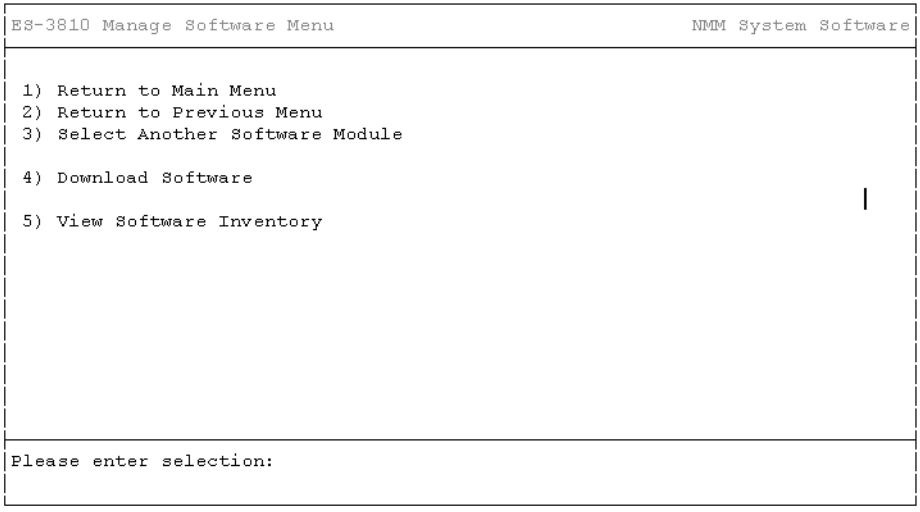


Figure 2.7 - Manage Software Menu

The items in the Manage Software Menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage System Menu.
Select Another Software Module	Returns to the Software Selection screen.
Download Software	Invokes the TFTP read utility to download an image containing the selected software module.
View Software Inventory	Displays the Software Inventory View screen.

2.1.3.1 Software Selection Menu

This menu asks the user to select a software module from a list of the software installed in the system. This screen is reached from the Main Menu through the Manage System Menu, then through the Manage Software option. After a valid software module ID is entered, the Manage Software Menu is displayed.

2.1.3.2 Downloading a New Software Image

For information about downloading a new software image to the ES-3810, see Chapter 4 of the *ForeRunner ES-3810 Installation and Maintenance Manual*.

2.1.3.3 Software Inventory View

This view is reached through the Manage System Menu, first by selecting the Manage Software option from the Manage System Menu and then by selecting the View Software Inventory option from the Manage Software Menu.

CHAPTER 3 Interface Management

This chapter details the menus used to manage the ES-3810's various interfaces. These menus are available by selecting the Manage Interface option from the ES-3810 Main Menu.

3.1 Selecting an Interface

To choose a specific interface, or group of interfaces, select the Manage Interface option from the Main Menu, then follow the guideline in the Interface Selection screen that appears (see Figure 3.1). After selecting an interface (or group of interfaces), you will be returned to the Manage Interface Menu which now displays the options available for the selected interface.

```
ES-3810 Interface Selection                    Interfaces D* (10BaseT Ethernet)

Interface  Description

 A1 - A2   100BaseTX Ethernet
 B1        OC-3c MM ATM
 C1 - C16  10BaseT Ethernet
 D1 - D24  10BaseT Ethernet
 F1        OC-3c MM ATM

 A*        All Interfaces in 2-port 100BaseTX Ethernet Switch Module
 C*        All Interfaces in 16 Port-10BaseTX Segment Switch Module
 D*        All Interfaces in 24-port 10BaseT Ethernet Switch Module

 *         All Ethernet Interfaces of ES3810

Please enter selection (by Interface):  _
```

Figure 3.1 - Interface Selection Screen

3.2 Managing 10 Mbps Ethernet Interfaces

This section explains how to view and manage the configuration of the 10Mbps Ethernet interfaces on the ESM-16 and the ESM-24. Figure 3.2 illustrates the Manage Interface Menu for the ESM-16 and ESM-24, which is reached by selecting a 10BaseT Ethernet interface from the Interface Selection menu.

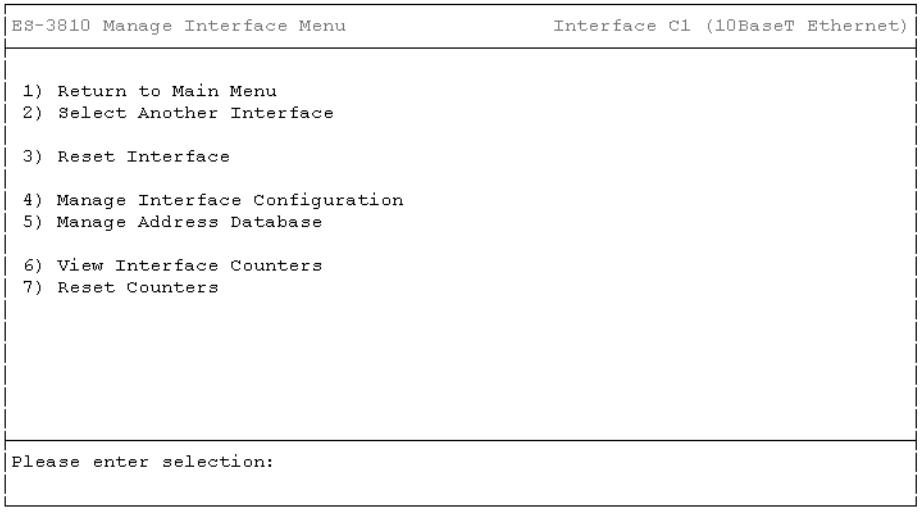


Figure 3.2 - ESM Manage Interface Menu

The items in the Manage Interface menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Select Another Interface	Returns to the Interface Selection menu.
Reset Interface	Resets the selected interface.
Manage Interface Configuration	Displays the Manage Interface Configuration Menu for the selected interface.
Manage Address Database	Displays the Manage Address Database Menu for the selected interface.
View Interface Counters	Displays the Interface Counters screen.
Reset Counters	Resets all counters for the selected interface.

3.2.1 Resetting the Interface

To reset the selected interface, select the Reset Interface option from the Manage Interface Menu (see Figure 3.2).

3.2.2 Manage Interface Configuration Menu

NOTE

10 Mbps segment interfaces are managed the same way as those on the ESM-16 and ESM-24, except that the address database can hold 8,192 addresses and each segment switch module supports a 4K bridge table.

This menu displays commands that provide access to managed objects that monitor and control the configuration for the selected interface. This menu is reached by selecting the Manage Interface Configuration option from the Manage Interface Menu (see Figure 3.3) for the ESMs. Figure 3.3 illustrates this menu.

```
ES-3810 Manage Configuration Menu              Interface D1 (10BaseT Ethernet)

 1) Return to Main Menu                 10) Half/Full Duplex Connection
 2) Return to Previous Menu             11) Internal Loopback

 3) View Configuration                  12) Work-Group/Backbone Connection

 4) Receiver                            13) Transmitter
 5) Polarity Correction                 14) Forced Transmits
 6) Sniffing                            15) Forward Sniffed Packets
 7) Sniffing Of Error Packets           16) Forward Flagged Packets
 8) Multicast Promiscuous Reception     17) Multicast Hash Upload
 9) Individual Promiscuous Reception

Please enter selection:
```

Figure 3.3 - ESM Manage Interface Configuration Menu

The items in the ESM Manage Interface Configuration Menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage Interface Menu.
View Configuration	Displays the Interface Configuration View screen for the selected interface.
Receiver	Queries the user to determine whether or not the interface's receiver is to be disabled or enabled.
Polarity Correction	Queries the user to determine whether or not the interface automatically corrects the polarity of the transmit and receive pairs comprising the physical medium.
Sniffing	Queries the user to determine whether or not the interface sniffs packets. Sniffing enables the forwarding of all transmitted and received packets onto the packet bus. In addition, the interface tags sniffed packets in order that other interfaces can forward them out of the system.
Sniffing of Error Packets	Queries the user to determine if the interface sniffs packets that have errors. If the interface is not sniffing, then this managed object has no relevance.

Multicast Promiscuous Reception	Queries the user to determine whether or not the interface promiscuously receives all multicast address packets.
Individual Promiscuous Reception	Queries the user to determine whether or not the interface promiscuously receives all individually addressed packets.
Half/Full Duplex Connection	Queries the user to determine if the interface is to provide half or full duplex connectivity.
Internal Loopback	Queries the user to determine whether or not the interface's internal loopback is to be enabled.
Work-Group/Backbone Connection	Queries the user to determine if the interface is to provide work-group or backbone connectivity.
Transmitter	Queries the user to determine whether or not the interface's transmitter is to be disabled or enabled.
Forced Transmits	Queries the user to determine whether or not the interface forces transmits when the link is not active.
Forward Sniffed Packets	Queries the user to determine whether or not the interface forwards sniffed packets out of the system.
Forward Flagged Packets	Queries the user to determine whether or not the interface forwards flagged packets out of the system.
Multicast Hash Upload	Queries the user to determine whether or not the interface accepts multicast hash upload packets.

3.2.2.1 Interface Configuration View

This view is reached by selecting the View Configuration option from the Manage Configuration Menu (see Figure 3.3) for the ESMs. Figure 3.4 illustrates the Interface Configuration View for 10Base interfaces.

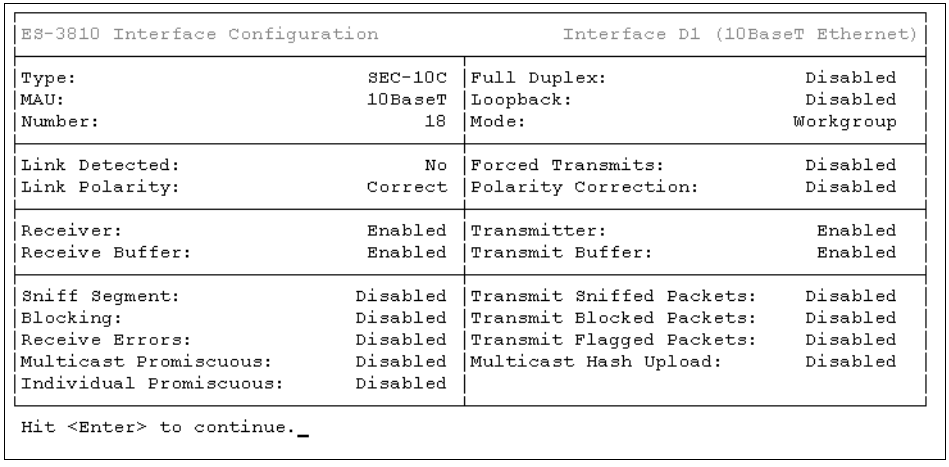


Figure 3.4 - ESM Interface Configuration View

3.2.3 Manage Address Database Menu

This menu is reached from the Main Menu through the Manage Interface menu (see Figure 3.2) by selecting the Manage Address Database option. This menu displays commands that provide access to managed objects that monitor and control the address database associated with the selected interface. Figure 3.5 illustrates the Manage Address Database Menu.

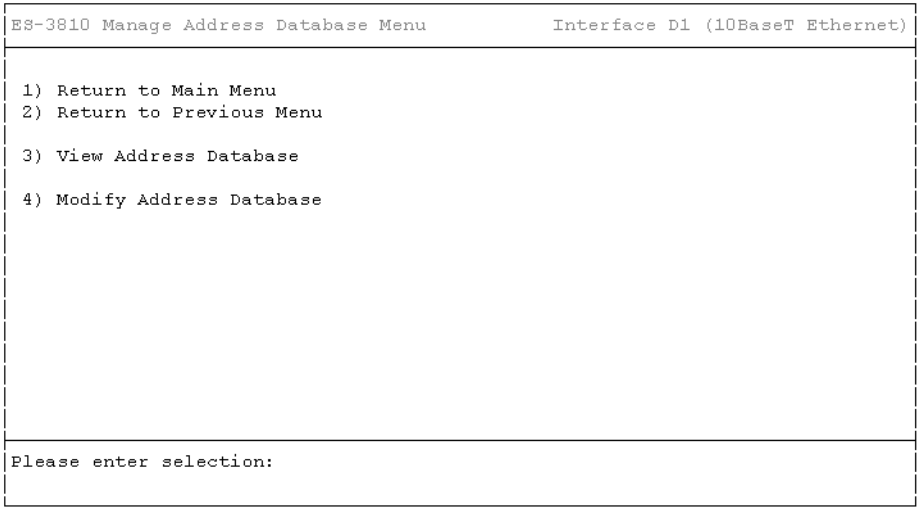


Figure 3.5 - ESM Manage Address Database Menu

The items in the ESM Manage Address Database menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage Interface Menu.
View Address Database	Displays the Address Database View screen for the selected interface.
Modify Address Database	Displays the list of entries in the address database and asks the user to select one to be modified. Next, the user is asked to modify the MAC address, age, multicast mask, and flag values for the entry.

3.2.3.1 Address Database View

This menu is reached from the Manage Interface menu (see Figure 3.2) then through the Manage Address Database Menu (see Figure 3.5) by selecting the View Address Database option. Figure 3.6 illustrates the Address Database View screen.

```
ES-3810 Address Database                          Interface D1 (10BaseT Ethernet)

| Entry | Address           | Age     | Multicast Mask        | Flagged |
|-------|-------------------|---------|-----------------------|---------|
| 1     | ----------------- | invalid | 1111 1111 1111 1111 | ---     |
| 2     | ----------------- | invalid | 1111 1111 1111 1111 | ---     |
| 3     | ----------------- | invalid | 1111 1111 1111 1111 | ---     |
| 4     | ----------------- | invalid | 1111 1111 1111 1111 | ---     |

=>
Commands:  +, -, Freeze, Unfreeze, Quit
```

Figure 3.6 - ESM Address Database View for Current Configuration

3.2.3.2 Modify Address Database Menu

This menu is reached from the Manage Interface menu (see Figure 3.2) then through the Manage Address Database Menu (see Figure 3.5) by selecting the Modify Address Database option. Figure 3.6 illustrates the Modify Address Database screen.

```
ES-3810 Modify Address Database                    Interface D1 (10BaseT Ethernet)

| Entry | Address           | Age     | Multicast Mask      | Flagged |
|-------|-------------------|---------|---------------------|---------|
| 1     | ----------------- | invalid | 1111 1111 1111 1111 | ---     |
| 2     | ----------------- | invalid | 1111 1111 1111 1111 | ---     |
| 3     | ----------------- | invalid | 1111 1111 1111 1111 | ---     |
| 4     | ----------------- | invalid | 1111 1111 1111 1111 | ---     |

 Which entry do you want to modify (1-4):  1

Address [-----------------]:  00-00-00-00-00-01
Age [invalid]:  valid
Flag [No ]:  No
```

Figure 3.7 - ESM Modify Address Database Menu

3.2.4 Viewing Interface Counters

This menu is reached from the Main Menu through the Manage Interface menu (see Figure 3.2) by selecting the View Interface Counters option. Figure 3.8 illustrates the Interface Counters screen for the interfaces supported by an ESM-16 and ESM-24.

```
ES-3810 Interface D1 (10BaseT Ethernet) Counters                  2:14:51.80

        Transmit Counters                       Receive Counters
Octets:                              0   Octets:                          0
Packets:                             0   Packets:                         0
Lost Packets:                        0   Lost Packets:                    0
Broadcasts:                          0   Broadcasts:                      0
Multicasts:                          0   Multicasts:                      0
Initially Deferred:                  0   Short Packets:                   0
Single Collisions:                   0   Long Packets:                    0
Multiple Collisions:                 0   Framing Errors:                  0
Excessive Collisions:                0   FCS Errors:                      0
Late Collisions:                     0
Carrier Lost:                        0

                        Packet Size Histogram
     64          65-127       128-255      256-511      512-1024      >1024
          0            0            0            0            0            0

=> _
Commands:  +, -, Freeze, Unfreeze, Quit
```

Figure 3.8 - ESM Interface Counters View

3.2.5 Resetting Interface Counters

To reset the counters of the selected interface, select the Reset Counters option from the Manage Interface Menu (see Figure 3.2).

3.3 Managing 10/100Mbps Ethernet Interfaces

This section details the menus used to manage the interfaces on the ES-3810's Fast Ethernet Modules (FEMs). Figure 3.9 illustrates the Manage Interface Menu for the FEMs.

```
ES-3810 Manage Interface Menu                Interface C1 (100BaseTX Ethernet)

 1) Return to Main Menu
 2) Select Another Interface

 3) Reset Interface

 4) Manage Interface Configuration
 5) Manage Address Database

 6) View Interface Counters
 7) Reset Counters

Please enter selection:
```

Figure 3.9 - FEM Manage Interface Menu

The items in the FEM Manage Interface menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Select Another Interface	Returns to the Interface Selection menu.
Reset Interface	Resets the selected interface.
Manage Interface Configuration	Displays the Manage Interface Configuration Menu for the selected interface.
Manage Address Database	Displays the Manage Address Database Menu for the selected interface.
View Interface Counters	Displays the Interface Counters screen.
Reset Counters	Resets all counters for the selected interface.

3.3.1 Resetting the Interface

To reset the selected interface, select the Reset Interface option from the Manage Interface Menu (see Figure 3.9).

3.3.2 Manage Configuration Menu

10/100 Mbps segment interfaces are managed the same way as those on other FEMs, except that the address database can hold 8,192 addresses.

This menu displays commands that provide access to managed objects that monitor and control the configuration for the selected 10/100 Mbps interface. This menu is reached by selecting Manage Interface Configuration option from the Manage Interface Menu (see Figure 3.9). Figure 3.10 illustrates the Manage Configuration menu for 10/100 Mbps interfaces.

```
ES-3810 Manage Configuration Menu            Interface A1 (100BaseTX Ethernet)

 1) Return to Main Menu                 9) Media Configuration
 2) Return to Previous Menu            10) Internal Loopback
                                       11) Work-Group/Backbone Connection
 3) View Configuration                 12) IA Domain Matching

 4) Receiver                           13) Transmitter

 5) Sniffing                           14) Forward Sniffed Packets
 6) Sniffing Of Error Packets          15) Forward Flagged Packets
 7) Multicast Promiscuous Reception    16) Multicast Hash Upload
 8) Individual Promiscuous Reception
                                       17) Dump ICS1890 Registers

Please enter selection:  _
```

Figure 3.10 - FEM Manage Configuration Menu

The items in the Manage Configuration menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage Interface Menu.
View Configuration	Displays the Interface Configuration View screen for the selected interface.
Receiver	Queries the user to determine whether or not the interface's receiver is to be disabled or enabled.
Sniffing	Queries the user to determine whether or not the interface sniffs packets. Sniffing enables the forwarding of all transmitted and received packets onto the packet bus. In addition, the interface tags sniffed packets in order that other interfaces can forward them out of the system.
Sniffing of Error Packets	Queries the user to determine whether or not the interface sniffs packets that have errors. If the interface is not sniffing, then this managed object has no relevance.
Multicast Promiscuous Reception	Queries the user to determine whether or not the interface promiscuously receives all multicast address packets.
Individual Promiscuous Reception	Queries the user to determine whether or not the interface promiscuously receives all individually addressed packets.

Media Configuration	Displays the current state of the auto-negotiated connection.
Internal Loopback	Queries the user to determine if the interface's internal loopback is to be disabled or enabled.
Work-Group/Backbone Connection	Queries the user to determine if the interface is to provide work-group or backbone connectivity.
IA Domain Matching	Queries the user to determine if individual address domain matching will be enabled.
Transmitter	Queries the user to determine whether or not the interface's transmitter is to be disabled or enabled.
Forward Sniffed Packets	Queries the user to determine whether or not the interface forwards sniffed packets out of the system.
Forward Flagged Packets	Queries the user to determine whether or not the interface forwards flagged packets out of the system.
Multicast Hash Upload	Queries the user to determine whether or not the interface accepts multicast hash upload packets.
Dump ICS1890 Registers	Displays the values of the registers associated with the selected port.

3.3.2.1 Interface Configuration View

This view is reached through the Manage Interface Menu (see Figure 3.9) and then through the Manage Configuration Menu (see Figure 3.10) by selecting the View Configuration option. Figure 3.11 illustrates the Interface Configuration View for 10/100 Mbps-based interfaces.

```
ES-3810 Interface Configuration              Interface A1 (100BaseTX Ethernet)

Type:                              SEC-100C  Loopback:                    Disabled
MAU:                             100BaseTX   Mode:                        Workgroup
Number:                                  0

Media Configuration:  Auto-Negotiation In Progress

Link Detected:                           No  VLAN Extension:                     n/a
IA Domain Matching:                Disabled  Multicast Filtering:                n/a

Receiver:                           Enabled  Transmitter:                     Enabled
Receive Buffer:                     Enabled  Transmit Buffer:                 Enabled

Sniff Segment:                     Disabled  Transmit Sniffed Packets:      Disabled
Receive Errors:                    Disabled  Transmit Flagged Packets:      Disabled
Multicast Promiscuous:             Disabled  Multicast Hash Upload:         Disabled
Individual Promiscuous:            Disabled

Hit <Enter> to continue.
```

Figure 3.11 - Interface Configuration View

3.3.3 Manage Address Database Menu

This menu is reached from the Main Menu through the Manage Interface menu (see Figure 3.9) by selecting the Manage Address Database option. This menu displays commands that provide access to managed objects that monitor and control the address database associated with the selected 10/100 Mbps interface. Figure 3.12 illustrates the Manage Address Database Menu.

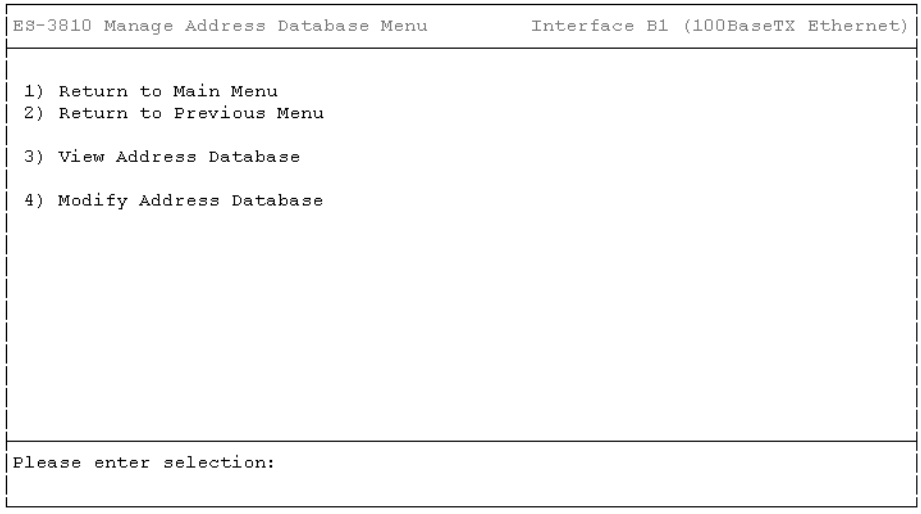


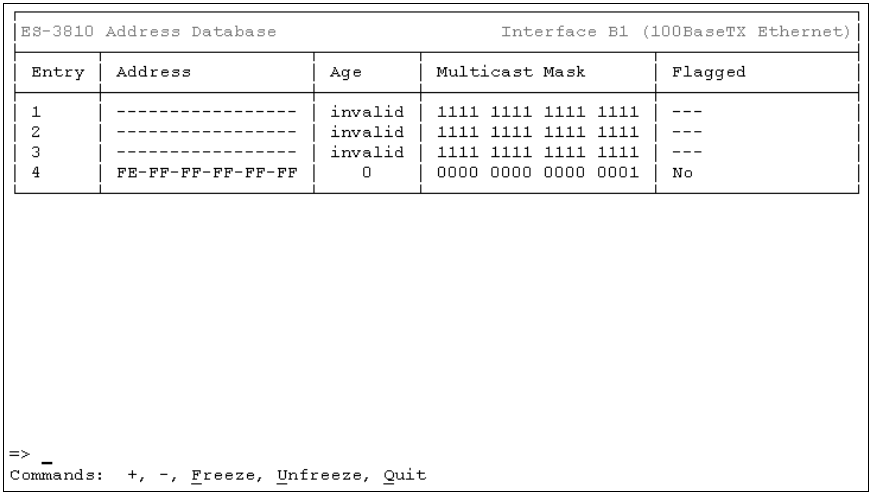
Figure 3.12 - Manage Address Database Menu

The items in the FEM Manage Address Database menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage Interface Menu.
View Address Database	Displays the Address Database View screen for the selected interface.
Modify Address Database Entry	Displays the list of entries in the address database and asks the user to select one to be modified. Next, the user is asked to modify the MAC address, age, multicast mask, and flag values for the entry.

3.3.3.1 Address Database View

This menu is reached from the Manage Interface menu (see Figure 3.9) then through the Manage Address Database Menu (see Figure 3.12) by selecting the View Address Database option. Figure 3.13 illustrates the Address Database View screen.



ES-3810 Address Database — Interface B1 (100BaseTX Ethernet)

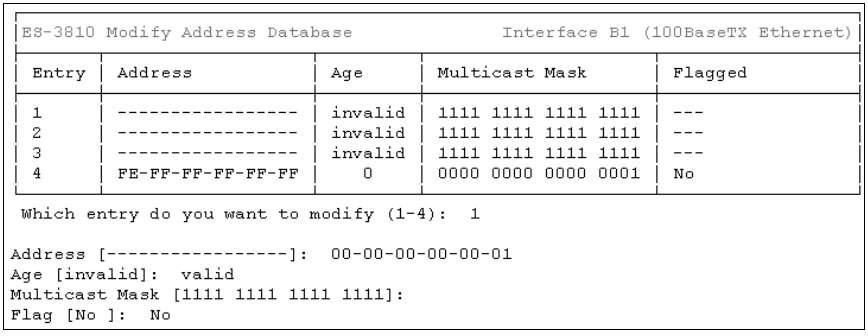
Entry	Address	Age	Multicast Mask	Flagged
1	----------	invalid	1111 1111 1111 1111	---
2	----------	invalid	1111 1111 1111 1111	---
3	----------	invalid	1111 1111 1111 1111	---
4	FE-FF-FF-FF-FF-FF	0	0000 0000 0000 0001	No

=> _
Commands: +, -, Freeze, Unfreeze, Quit

Figure 3.13 - Address Database View

3.3.3.2 Modify Address Database Menu

This menu is reached from the Manage Interface menu (see Figure 3.9) then through the Manage Address Database Menu (see Figure 3.12) by selecting the Modify Address Database option. Figure 3.14 illustrates the Address Database Entry Selection screen.



ES-3810 Modify Address Database — Interface B1 (100BaseTX Ethernet)

Entry	Address	Age	Multicast Mask	Flagged
1	----------	invalid	1111 1111 1111 1111	---
2	----------	invalid	1111 1111 1111 1111	---
3	----------	invalid	1111 1111 1111 1111	---
4	FE-FF-FF-FF-FF-FF	0	0000 0000 0000 0001	No

Which entry do you want to modify (1-4): 1

Address [----------]: 00-00-00-00-00-01
Age [invalid]: valid
Multicast Mask [1111 1111 1111 1111]:
Flag [No]: No

Figure 3.14 - Modify Address Database Menu

3.3.4 Viewing Interface Counters

This view is reached from the Main Menu through the Manage Interface menu (see Figure 3.9) by selecting the View Interface Counters option. Figure 3.15 illustrates the View Interface Counters.

```
ES-3810 Interface B1 (100BaseTX Ethernet) Counters                  35:38.68

          Transmit Counters                      Receive Counters
Octets:                              0   Octets:                          0
Packets:                             0   Packets:                         0
Lost Packets:                        0   Lost Packets:                    0
Broadcasts:                          0   Broadcasts:                      0
Multicasts:                          0   Multicasts:                      0
Initially Deferred:                  0   Short Packets:                   0
Single Collisions:                   0   Long Packets:                    0
Multiple Collisions:                 0   Framing Errors:                  0
Excessive Collisions:                0   FCS Errors:                      0
Late Collisions:                     0
Carrier Lost:                        0

                          Packet Size Histogram
     64          65-127       128-255       256-511       512-1024       >1024
┌──────────┬──────────┬──────────┬──────────┬──────────┬──────────┐
│          0 │          0 │          0 │          0 │          0 │          0 │
└──────────┴──────────┴──────────┴──────────┴──────────┴──────────┘

=> _
Commands:  +, -, Freeze, Unfreeze, Quit
```

Figure 3.15 - Interface Counters View

3.3.5 Resetting Interface Counters

To reset the counters of the selected interface, select option **7** from the Manage Interface Menu.

3.4 Managing ATM Interfaces

This section details the menus used to manage the interfaces on the ES-3810's ATM interfaces.

3.4.1 Dual ATM Uplinks

The ES-3810 supports redundant ATM Uplinks. When two ATM Uplinks are installed in an ES-3810, they share the LECs created by the user. Odd-numbered LECs reside on the ATM uplink in the lower-numbered slot of the ES-3810 chassis. Even-numbered LECs reside on the ATM uplink in the higher-numbered slot in the ES-3810 chassis. For example, with ATM uplinks in slots B and C, the odd-numbered LECs reside on the uplink in slot B, and the even numbered LECs reside on the uplink in slot C. If one of the ATM uplinks fails, the ES-3810 will reconfigure the "failed" LECs on the other uplink.

An uplink "failure" is defined as uplink module failure or cut fiber.

3.4.2 Manage ATM Interface Menu

This menu displays commands that provide access to managed objects that monitor and control the selected interface. Figure 3.16 illustrates the Manage Interface Menu for ATM Uplink Modules.

```
ES-3810 Manage Interface Menu                    Interface A1 (OC-3c MM ATM)

 1) Return to Main Menu
 2) Select Another Interface

 3) Manage SONET/SDH Configuration
 4) Manage LANE Configuration
 5) Manage RFC1483 Connection
 6) Manage Signaling Configuration
 7) Manage ILMI Configuration

 8) View SONET Counters
 9) View ATM Counters
10) View AAL5 Counters
11) View LANE Counters
12) View LEC Counters
13) View Signaling Counters

Please enter selection: _
```

Figure 3.16 - Manage Interface Menu

The items in the previous menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Select Another Interface	Returns to the Interface Selection screen.
Manage SONET/SDH Configuration	Displays the Manage SONET/SDH Configuration Menu for the selected interface.
Manage LANE Configuration	Displays the Manage LANE Configuration Menu for the selected interface.
Manage RFC1483 Connection	Displays the Manage RFC1483 Connection Menu.
Manage Signaling Configuration	Displays the Manage Signaling Configuration Menu for the selected interface.
Manage ILMI Configuration	Displays the Manage ILMI Configuration Menu.
View SONET Counters	Displays the SONET Counters screen.
View ATM Counters	Displays the ATM Counters screen.
View AAL5 Counters	Displays the AAL5 Counters screen.
View LANE Counters	Displays the LANE Counters screen.
View LEC Counters	Displays the LEC Counters screen.
View Signaling Counters	Displays the Signaling Counters screen.

3.4.2.1 Manage SONET/SDH Configuration Menu

This menu displays commands that provide access to managed objects that monitor and control the SONET/SDH (Synchronous Optical NETwork / Synchronous Digital Hierarchy) configuration for the selected ATM based interface. This menu is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu. Figure 3.17 illustrates the Manage SONET/SDH Configuration Menu.

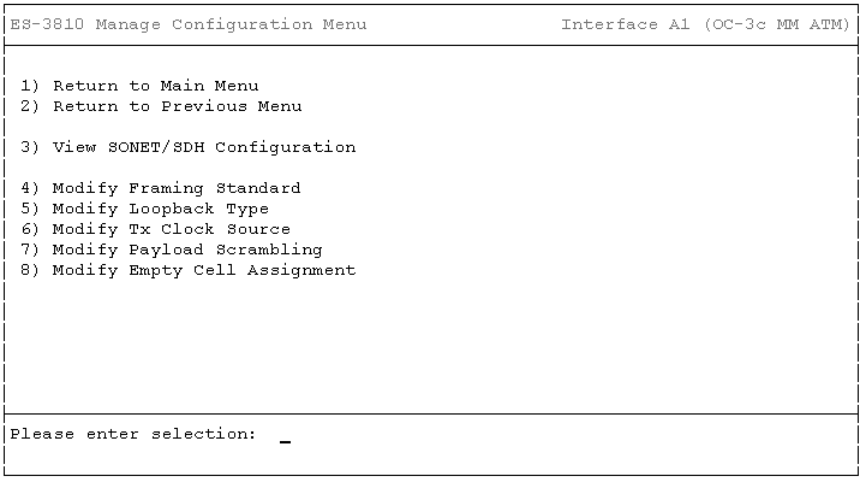


Figure 3.17 - Manage SONET/SDH Configuration Menu

The items in the previous menu have the following meanings:

Return to Main Menu — Returns to the Main Menu.

Return to Previous Menu — Returns to the Manage Interface Menu.

View SONET/SDH Configuration — Displays the SONET/SDH Configuration View screen for the selected interface.

Modify Framing Standard — Queries the user to determine the SONET/SDH framing standard to use. The current product supports two standards:

- SONET: North American defined Synchronous Optical NETwork (default)
- SDH: ITU defined Synchronous Digital Hierarchy

Modify Loopback Type — Queries the user to determine the loopback mode to use. The choices are:

- Line loopback
- Diagnostics loopback
- None (default)

Modify Tx Clock Source — Queries the user to determine what source for the Tx clock to use. The choices are:

- Internal (local) clock (default)
- Network (loop timing)

Modify Payload Scrambling — Queries the user to determine whether or not to enable payload scrambling. The default is Enabled.

Modify Empty Cell Assignment — Queries the user to determine the cell type to assign to empty cells. The choices are:

- ATM Forum UNI Unassigned Cell (default)
- ITU I.432 Idle Cell

3.4.2.1.1 SONET/SDH Configuration View

This menu is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu. Figure 3.18 illustrates the SONET/SDH Configuration View for ATM based interfaces.

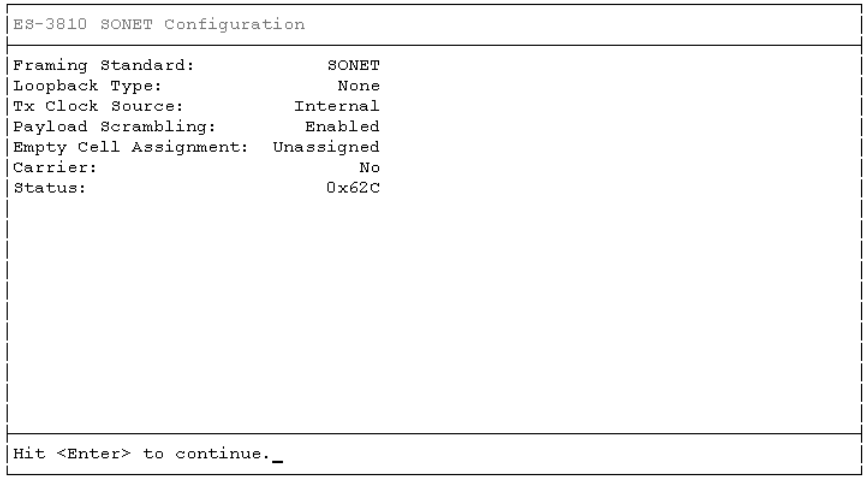


Figure 3.18 - SONET/SDH Configuration View

3.4.2.2 Manage LANE Configuration Menu

This menu displays commands that provide access to managed objects that monitor and control the LANE (LAN Emulation) configuration for the selected ATM interface. This menu is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu. Figure 3.19 illustrates the Manage LANE Configuration Menu.

```
ES-3810 Manage Configuration Menu                    Interface A1 (OC-3c MM ATM)

 1) Return to Main Menu
 2) Return to Previous Menu

 3) View LEC Configuration
 4) View LEC VCC List
 5) View LEC ARP Cache

 6) Create LEC
 7) Delete LEC

 8) Flush LEC ARP Cache

Please enter selection: _
```

Figure 3.19 - Manage LANE Configuration Menu

The items in the previous menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage Interface Menu.
View LEC Configuration	Displays the ELAN Selection screen and the LEC Configuration View screen for the selected ELAN.
View LEC VCC List	Displays the ELAN Selection screen and then the LEC VCC List screen for the selected ELAN.
View LEC ARP Cache	Displays the ELAN Selection screen and then the LEC ARP Cache screen for the selected ELAN.
Create LEC	Queries the user for the configuration of a new LEC.
Delete LEC	Displays the ELAN Selection screen and then asks the user if the selected LEC should be deleted.
Flush LEC ARP Cache	Displays the list of existing ELANs and asks the user for the ELAN whose LEC ARP cache is to be deleted.

3.4.2.2.1 LEC Configuration View

This view is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu then through the Manage LANE Configuration Menu. The user is then asked to select an ELAN to view. Figure 3.20 illustrates the LEC Configuration View.

```
ES-3810 LEC Configuration ELAN Id: 2

ELAN Name:               marketing
ELAN Id:                 2
LEC Id:                  0
Admin Status:            Up
Operational Status:      Waiting for Local Address
Selector:                0xFF
Mode:                    Automatic
LEC Address:             0x00.0000.00.000000.0000.0000.0000.000000000000.00
LECS Address:            0x47.0079.00.000000.0000.0000.0000.00A03E000001.00
LES Address:             0x00.0000.00.000000.0000.0000.0000.000000000000.00
BUS Address:             0x00.0000.00.000000.0000.0000.0000.000000000000.00
Config. Direct VCI:      None
Control Direct VCI:      None
Control Distribute VCI:  None
Multicast Send VCI:      None
Multicast Forward VCI:   None


Hit <Enter> to continue.
```

Figure 3.20 - LEC Configuration View

3.4.2.2.2 LEC VCC List

This screen lists all of the Virtual Channel Connections (VCCs) in use by a given LAN Emulation Client (LEC). This view is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu then through the Manage LANE Configuration Menu and finally through the ELAN Selection screen. Figure 3.21 illustrates the LEC VCC List screen for the selected ELAN.

```
ES-3810 VC List ELAN Id: 1

ELAN Id: 1, Elan Name: default
Index    VCI       VCI Type
   1     226       Config. Direct VCI
   2     227       Control Direct VCI
   3     228       Control Distribute VCI
   4     229       Multicast Send VCI
   5     230       Multicast Forward VCI
   6     231       Data Direct VCI

Hit <Enter> to continue.
```

Figure 3.21 - LEC VCC List View

3.4.2.2.3 LEC ARP Cache View

This screen lists all of the current ARP (Address Resolution Protocol) cache entries for the selected LAN Emulation Client (LEC). This view is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu then through the Manage LANE Configuration Menu and finally through the ELAN Selection screen. Figure 3.22 illustrates the LEC ARP Cache View screen for the selected ELAN.

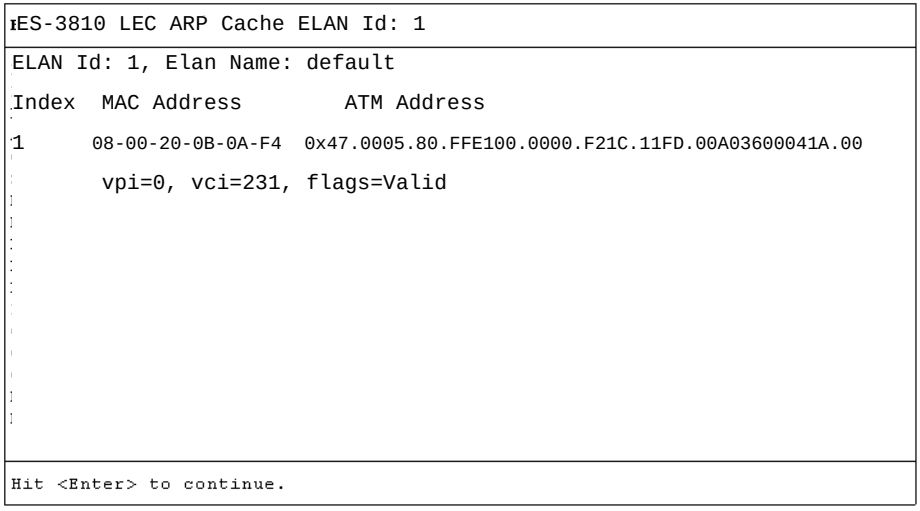


Figure 3.22 - LEC ARP Cache View

3.4.2.3 Manage RFC1483 Connection

This menu displays options that let the user view, create, and delete RFC 1483 Permanent Virtual Circuits (PVCs). PVCs act like ELANs on the ES-3810, in that you can associate VLANs to PVCs. The Manage RFC1483 Connection Menu is shown in Figure 3.23.

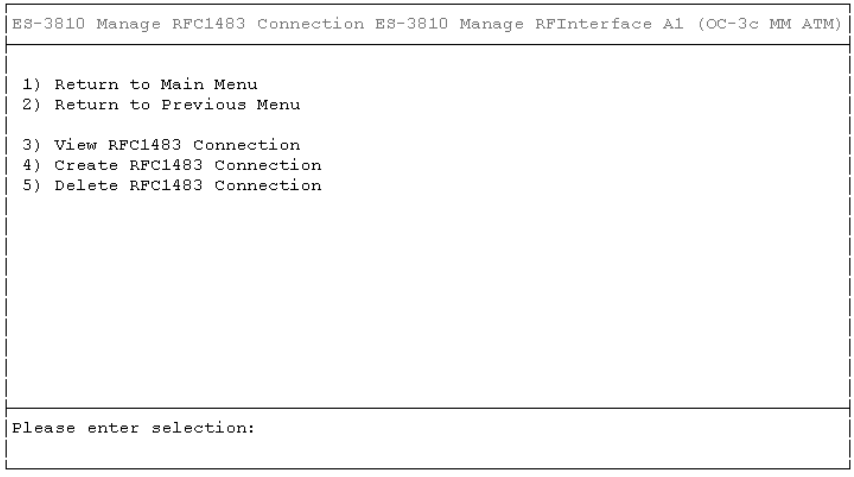


Figure 3.23 - Manage RFC1483 Connection Menu

3.4.2.3.1 View RFC1483 Connection

The View RFC1483 Connection Menu lets the user select a PVC and view its current configuration. To select a PVC, type **2** and press <ENTER> in the Manage RFC1483 Connection Menu. When the View RFC1483 Connection Menu appears, type the number that corresponds to the desired PVC and press <ENTER> (see Figure Figure 3.24). After selecting a PVC, it's connection parameters are displayed (see Figure 3.25).

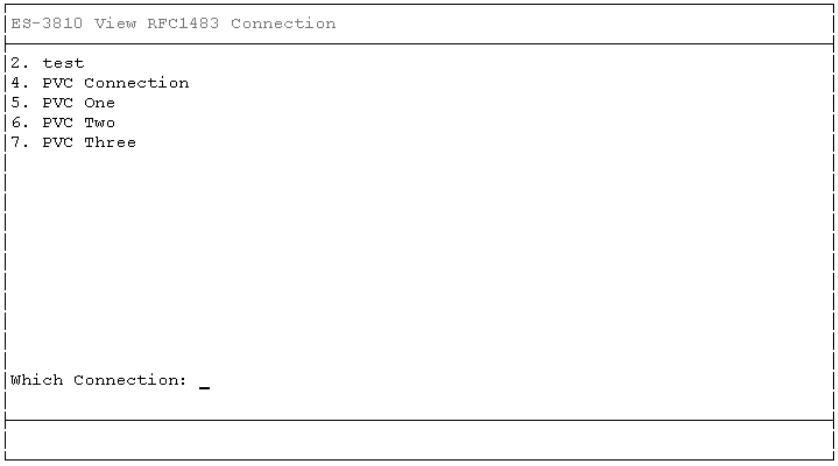


Figure 3.24 - View RFC1483 Connection Menu

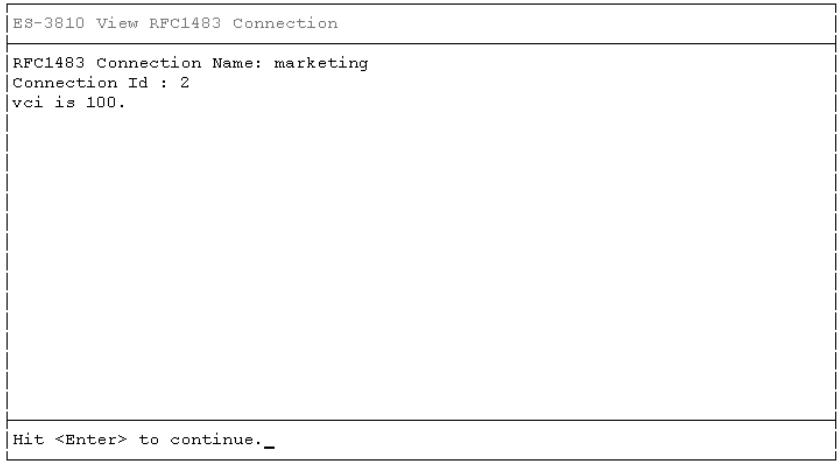


Figure 3.25 - View RFC1483 Connection

3.4.2.3.2 Create RFC1483 Connection

This menu lets the user create PVCs by choosing a name for the connection (ELAN) and a VCI value. To create a PVC, type **4** and press <ENTER> in the Manage RFC1483 Connection Menu. When prompted, type the name of the connection and press <ENTER>, type in the VCI value for the connection and press <ENTER>.

After entering the VCI for the connection, you are prompted to confirm the settings you just entered. If you are satisfied with the settings, type **y** and press <ENTER>. If you are not satisfied with the settings, type **n** and press <ENTER>. After accepting or declining your choices, press <ENTER> again (see Figure 3.26).

```
ES-3810 Create RFC1483 Connection

Configuring a new RFC1483 Connection...

Enter Connection Name : marketing
Enter VCI: 150

RFC1483 Connection Name: marketing
vci is 150.
Are you satisfied with these settings [No]?  y

RFC 1483 Connection  Configured. (ELAN ID : 8)
Connection Name: marketing
PVC Number: 150




  Hit <Enter> to continue._
```

Figure 3.26 - Creating a PVC

3.4.2.3.3 Delete RFC1483 Connection

This menu lets the user delete PVCs. To delete PVCs, type **5** and press <ENTER> in the Manage RFC1483 Connection Menu. When the Delete RFC1483 Connection Menu appears, type the number that corresponds to the PVC to be deleted and press <ENTER> (see Figure 3.27).

```
ES-3810 Delete RFC1483 Connection

2. marketing
7. testing
8. pubs
9. graphics

Which Connection: 2
```

Figure 3.27 - Selecting a PVC to Delete

You are asked to confirm your choice. If you still wish to delete the PVC, type **y** and press <ENTER>. If you do not wish to delete the PVC, type **n** and press <ENTER>. After confirming your choice, press <ENTER> (see Figure 3.28).

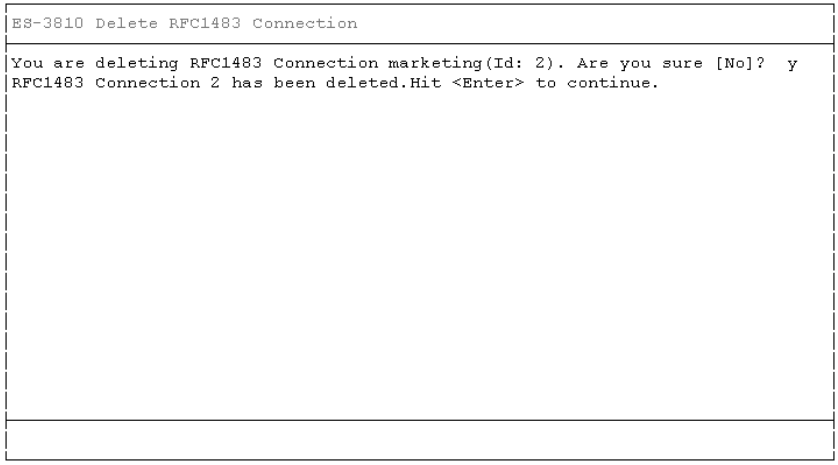


Figure 3.28 - Confirming the Deletion of a PVC

3.4.2.4 Manage Signaling Configuration Menu

This menu displays commands that provide access to managed objects that monitor and control the signaling configuration for the selected ATM interface. This menu is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu. Figure 3.23 illustrates the Manage Signaling Configuration Menu.

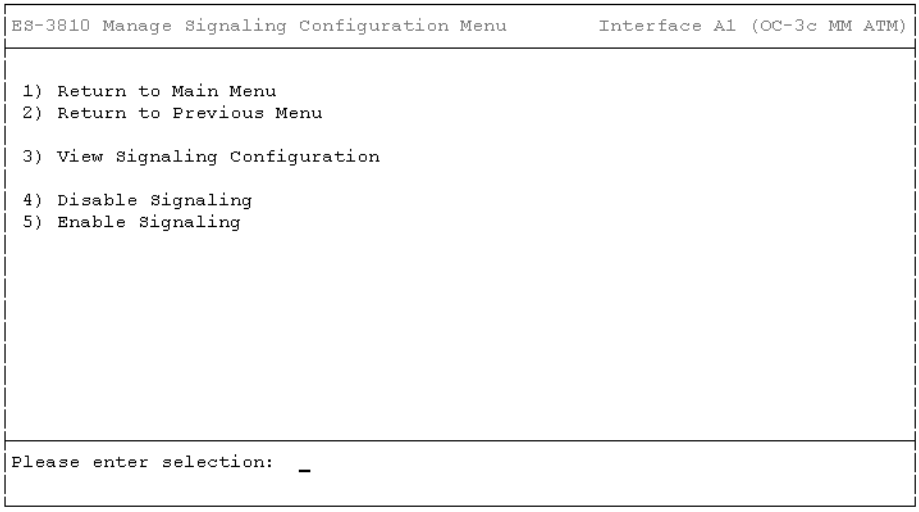


Figure 3.29 - Manage Signaling Configuration Menu

The items in the previous menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage Interface Menu.
View Signaling Configuration	Displays the Signaling Configuration View screen for the selected interface.
Disable Signaling	Attempts to disable signaling, but asks for user confirmation before doing so.
Enable Signaling	Attempts to enable signaling, but asks for user confirmation before doing so.

3.4.2.4.1 Signaling Configuration View

This view is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu and then through the Manage Signaling Configuration Menu. Figure 3.24 illustrates the Signaling Configuration View.

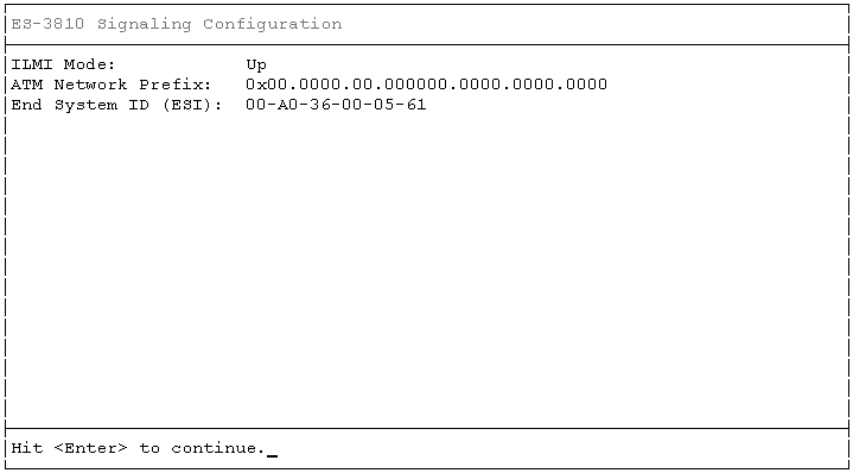


Figure 3.30 - Signaling Configuration View

3.4.2.5 Manage ILMI Configuration

This menu lets the user manage ILMI on the ATM interface of the ES-3810. To manage ILMI, type **7** and press <ENTER> in the Manage Interface Menu. The Manage ILMI Configuration Menu appears (see Figure 3.31).

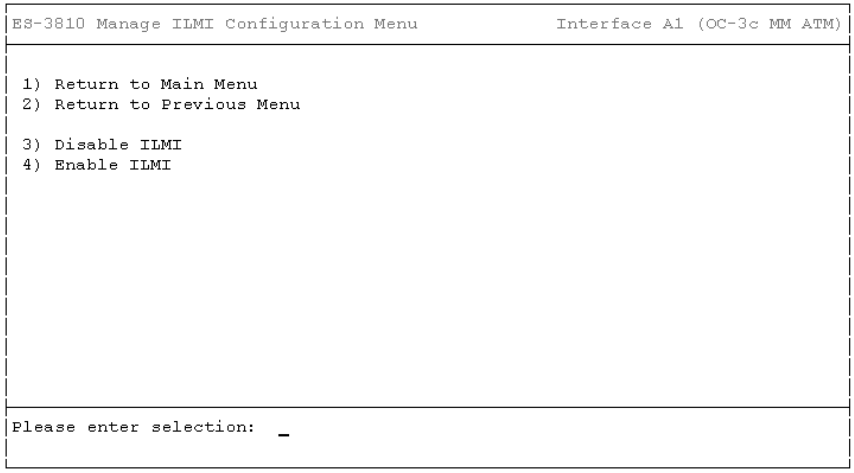


Figure 3.31 - Manage ILMI Configuration Menu

3.4.2.5.1 Disabling ILMI

To disable ILMI on the selected ATM interface, type 3 and press <ENTER> in the Manage ILMI Configuration Menu.

NOTE

You can not disable ILMI until you have delete all the ELANs on the ES-3810. Delete LANE ELANs from the Manage LANE Configuration Menu. Delete PVC ELANs from the Manage RFC1483 Connection Menu.

Once you have deleted all ELANs on the ES-3810, you can disable ILMI. After entering **3** in the Manage ILMI Configuration Menu, you are prompted to confirm you choice to disable ILMI. If you still wish to disable ILMI, type **y** and press <ENTER>. If you do not wish to disable ILMI, type **n** and press <ENTER>. After confirming whether or not to disable ILMI, press <ENTER> again (see Figure 3.32).

```
ES-3810 Disable ILMI

Are you sure to disable ilmi [No]?  y
ILMI has been disabled.Hit <Enter> to continue._
```

Figure 3.32 - Disabling ILMI

3.4.2.5.2 Enabling ILMI

To enable ILMI on the selected ATM interface, type **4** and press <ENTER> in the Manage ILMI Configuration Menu. When prompted to confirm your choice type **y** and press <ENTER> if you still wish to enable ILMI. If you do not wish to enable ILMI, type **n** and press <ENTER>. After confirming whether or not to enable ILMI, press <ENTER> again (see Figure 3.33).

```
ES-3810 Enable ILMI

Are you sure to enable ILMI [No]?  y
ILMI has been enabled.Hit <Enter> to continue.
```

Figure 3.33 - Enabling ILMI

3.4.2.6 View SONET Counters

This view is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu. Figure 3.34 illustrates the SONET Counters screen for interfaces supported by an ATM module.

```
ES-3810 SONET Counters                                          3:50.22

Section BIPs                12274032
Section LOSs                     255
Section LOFs                     255
Line BIPs                         24
Line FEBEs                        23
Line AISs                        255
Line FERFs                         0
Path BIPs                         14
Path FEBEs                         3
Path LOPs                          0
Path AISs                        255
Path Yellows                     255
Correctable HCSs                   0
Uncorrectable HCSs                 0




=>
Commands:  +, -, Freeze, Unfreeze, Quit
```

Figure 3.34 - SONET Counters View

3.4.2.7 View ATM Counters

This view is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu. Figure 3.35 illustrates the ATM Counters screen for interfaces supported by an ATM module.

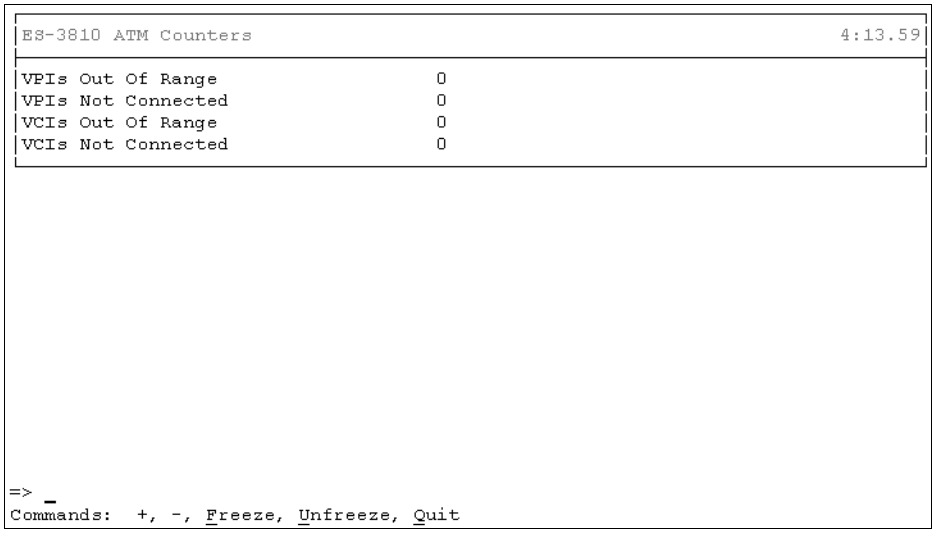


Figure 3.35 - ATM Counters View

3.4.2.8 View AAL5 Counters

This view is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu. Figure 3.36 illustrates the AAL5 Counters screen for interfaces supported by an ATM module.

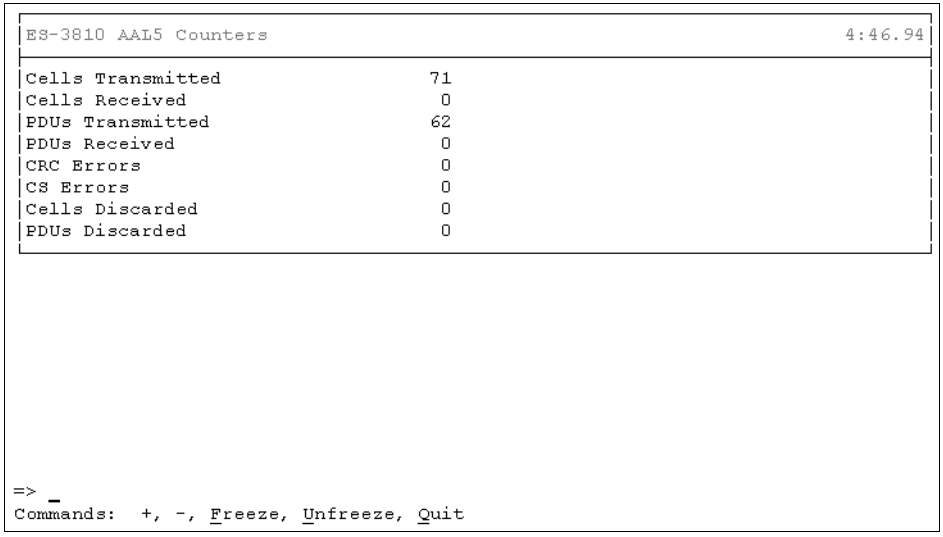


Figure 3.36 - AAL5 Counters View

3.4.2.9 View LANE Counters

This view is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu. Figure 3.37 illustrates the LANE Counters screen for interfaces supported by an ATM module.

```
ES-3810 LANE Counters                                              5:16.15

Total Bytes to ATM:                 0
Total Bytes to Ethernet:            0
Cells to Ethernet Dropped:          0
Packets to ATM Dropped:             0
Packets From ATM Dropped:           0
Wrong Size ATM PDUs:                0
Wrong Size Ethernet Frames:         0
Echo Suppressions:                  0
Invalid VCC Accessed:               0
Limits to BUS Exceeded:             0
Unrecognized Ethernet Frames:       0

=> _
Commands:  +, -, Freeze, Unfreeze, Quit
```

Figure 3.37 - LANE Counters View

3.4.2.10 View LEC Counters

This view is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu. Figure 3.38 illustrates the LEC Counters screen for interfaces supported by an ATM module.

```
ES-3810 ELAN 3 (Engineering) LEC Counters                  1 18:51:39.15

SVC Failures:                        0
Control Packets Received:            0
Control Packets Sent:                0
ARP Replies Received:                0
ARP Replies Sent:                    0
ARP Requests Received:               0
ARP Requests Sent:                   0
Join Calls:                          0
Topology Change Indications:         0

Hit <Enter> to continue.
```

Figure 3.38 - LEC Counters View

3.4.2.11 View Signaling Counters

This view is reached from the Main Menu through the Interface Selection screen then through the Manage Interface Menu. Figure 3.39 illustrates the Signaling Counters screen for interfaces supported by an ATM module.

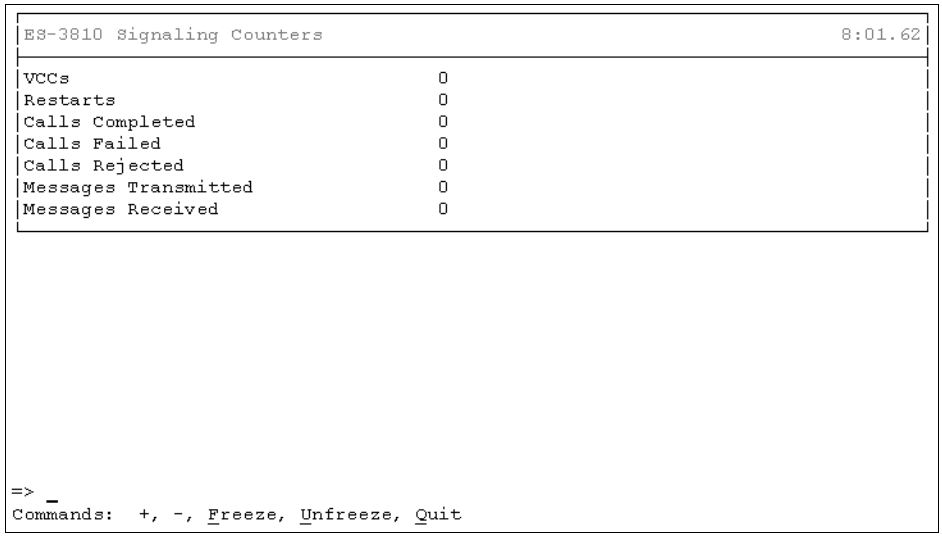


Figure 3.39 - Signaling Counters View

CHAPTER 4 VLAN Management

This chapter provides information about managing virtual LANs (VLANs) on the ES-3810. For more information about using VLANs, see Appendix A in the *ForeRunner ES-3810 Installation and Maintenance Manual.*

4.1 Manage VLAN Menu

This menu displays commands that provide access to managed objects that monitor and control the VLANs. This menu is reached from the Main Menu through the Manage VLAN option. Figure 4.1 illustrates the Manage VLAN Menu.

```
ES-3810 Manage VLAN Menu                                VLAN 1 (default)

 1) Return to Main Menu
 2) Select Another VLAN

 3) View VLAN
 4) Create VLAN
 5) Modify VLAN
 6) Delete VLAN
 7) Rename VLAN

 8) View VLAN Inventory

Please enter selection:
```

Figure 4.1 - Manage VLAN Menu

The items in the previous menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Select Another VLAN	Returns to the VLAN Selection Menu.
View VLAN	Displays the VLAN View screen for the selected VLAN.

Create VLAN	Queries the user for the name of the new VLAN, the ports that are to belong to that VLAN, whether or not IP multicast filtering is to be enabled, a MAC address to add to the VLAN, whether or not to join the new VLAN, the configuration (“auto” or “manual”), and whether or not to use the default LECS address.
Modify VLAN	Displays the VLAN Selection screen and then queries the user for a new name for the selected VLAN and new ports that are to belong to that VLAN.
Delete VLAN	Displays the Delete VLAN Menu and queries the user for the number of the VLAN to be deleted.
Rename VLAN	Displays the Rename VLAN Menu and queries the user for the number of the VLAN to be renamed.
View VLAN Inventory	Displays the VLAN Inventory View screen.

4.1.1 Modify VLAN Menu

Selecting Modify VLAN from the Manage VLAN Menu, causes the Modify VLAN menu being displayed (see Figure 4.2).

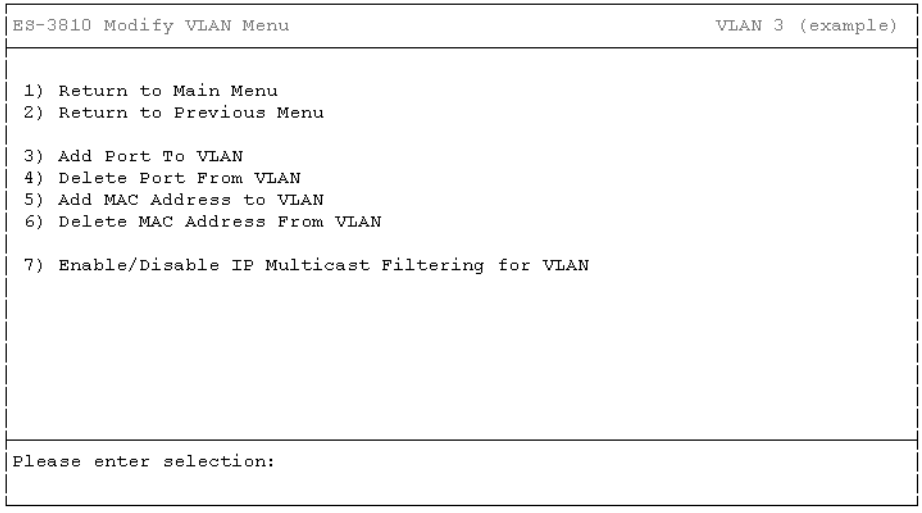


Figure 4.2 - Modify VLAN Menu

The items in the previous menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage VLAN Menu.
Add Port to VLAN	Queries the user for the port(s) to add to the selected VLAN and whether or not IP multicast filtering is to be enabled.
Delete Port from VLAN	Queries the user for the port(s) to be deleted from the selected VLAN.
Add MAC Address to VLAN	Queries the user for the MAC address(es) to be added to the selected VLAN.
Delete MAC Address from VLAN	Queries the user for the MAC address(es) to be deleted from the selected VLAN.
Enable/Disable IP Multicast Filtering for VLAN	Asks the user whether to enable or disable IP multicast filtering.

4.1.2 VLAN Selection Menu

Selecting Select Another VLAN from the Manage VLAN Menu, causes the VLAN Selection menu being displayed (see Figure 4.3). This menu prompts for a VLAN from a list of the VLANs defined in the system. Until VLANs are defined, only the default is available.

```
ES-3810 VLAN Selection                                    VLAN 1 (default)

Number | Name
-------+-------------------------------------------------------------------
   1   | default
   2   | pubs
-------+-------------------------------------------------------------------
Please enter selection (by Number):  2
```

Figure 4.3 - VLAN Selection Menu

4.1.2.1 VLAN View

Selecting View VLAN from the Manage VLAN Menu, causes the View VLAN screen being displayed (see Figure 4.4).

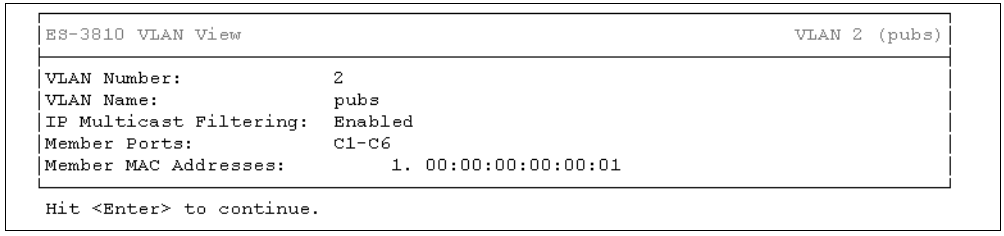


Figure 4.4 - VLAN View

4.1.3 VLAN Inventory View

Selecting View VLAN Inventory from the Manage VLAN Menu, causes the View VLAN Inventory screen being displayed (see Figure 4.5).

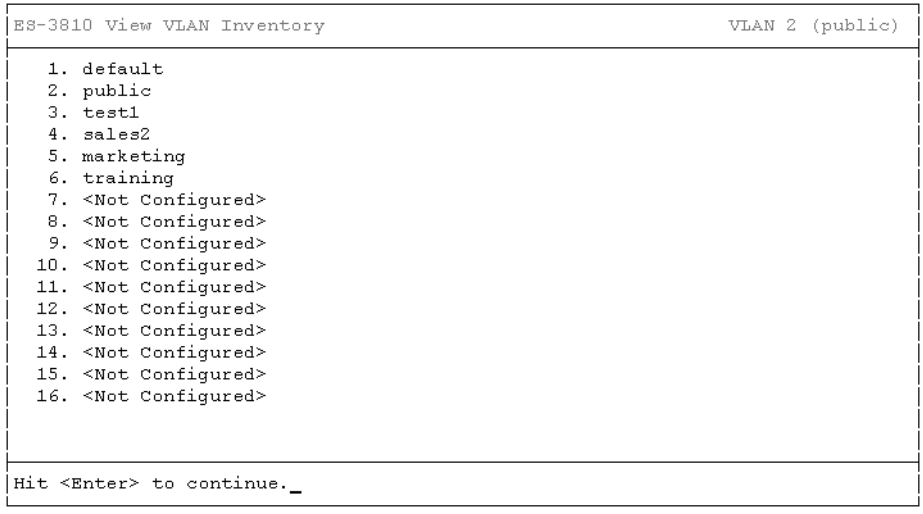


Figure 4.5 - VLAN Inventory View

CHAPTER 5 UDP/IP Management

This chapter describes the menus used to access and configure managed objects that monitor and control the UDP / IP stack.

5.1 Manage UDP/IP Menu

This menu is reached directly from the Main Menu by selecting the Manage UDP / IP option. Figure 5.1 illustrates the Manage UDP / IP Menu.

```
ES-3810 Manage UDP/IP Menu

 1) Return to Main Menu

 2) Manage ARP Cache
 3) Manage IP Parameters
 4) Manage IP Route Table

 5) View ICMP Counters
 6) View IP Counters
 7) View UDP Counters

 8) Ping

Please enter selection:
```

Figure 5.1 - Manage UDP / IP Menu

The items in the Manage UDP/IP menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Manage ARP Cache	Displays the Manage ARP Cache Menu.
Manage IP Parameters	Displays the Manage IP Parameters Menu.
Manage IP Routing Table	Displays the Manage IP Routing Table Menu.
View ICMP Counters	Displays the ICMP Counters screen.
View IP Counters	Displays the IP Counters screen.
View UDP Counters	Displays the UDP Counters screen.

5.1.1 Manage ARP Cache Menu

This menu displays commands that provide access to managed objects that monitor and control the ARP cache. This menu is reached from the Main Menu through the Manage UDP/IP Menu (see Figure 5.1) by selecting the Manage ARP Cache option. Figure 5.2 illustrates the Manage ARP Cache Menu.

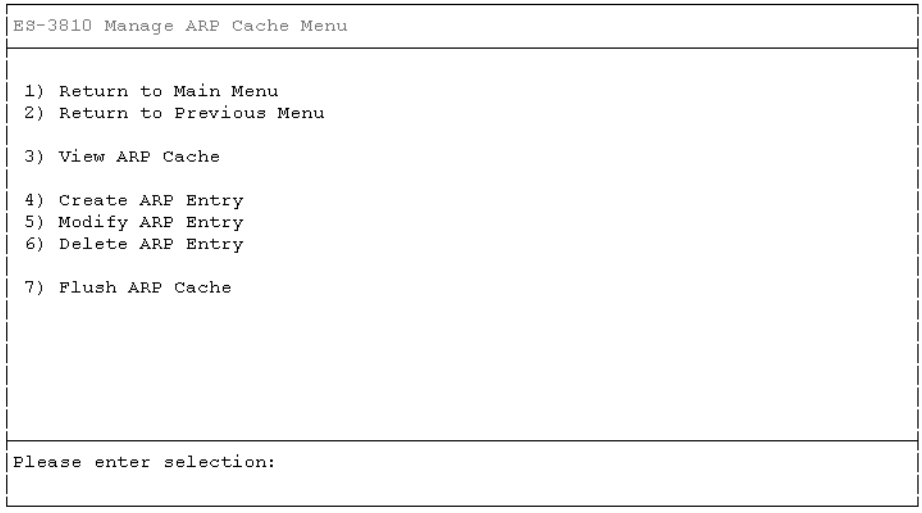


Figure 5.2 - Manage ARP Cache Menu

The items in the Manage ARP Cache Menu have the following meanings:

Return to Main Menu Returns to the Main Menu.

Return to Previous Menu Returns to the Manage UDP/IP Menu.

View ARP Cache Displays the ARP Cache View screen.

Create ARP Entry Queries the user for an IP address and an associated physical address. If the information provided by the user is valid, an entry does not already exist with the specified IP address, and the ARP cache is not full, then the management console adds an entry to the ARP cache. If the ARP entry could not be added to the ARP cache, then the management console displays an appropriate error message.

Entries added to the ARP cache through the management console always have a fixed state. The management console considers ARP cache entries with the fixed state part of the system's configuration, thereby making them persistent.

Modify ARP Entry Queries the user for an IP address. If the information provided by the user is valid, and the specified entry exists in the ARP cache, then the management console asks the user for a new physical address. If the specified entry does not exist in the ARP cache, then the management console displays an appropriate error message.

Delete ARP Entry Queries the user for an IP address. If the information provided by the user is valid, and the specified entry exists in the ARP cache, then the management console deletes the specific entry from the ARP cache. The management console confirms the action. If the specified entry does not exist in the ARP cache, then the management console displays an appropriate error message.

Flush ARP Cache Deletes all entries that do not have a fixed state from the ARP cache. The management console explains and confirms this action with the user.

5.1.1.1 ARP Cache View

This view is reached through the Manage UDP/IP Menu (see Figure 5.1), then through the Manage ARP Cache Menu (see Figure 5.2) by selecting the View ARP Cache option. Figure 5.3 illustrates the ARP Cache View screen.

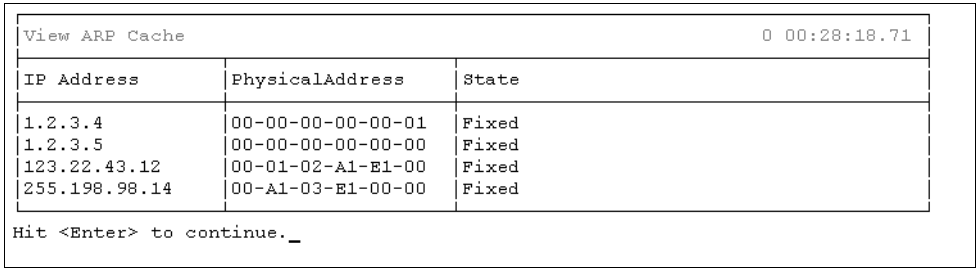


Figure 5.3 - ARP Cache View

5.1.2 Manage IP Parameters Menu

This menu displays commands that provide access to managed objects that monitor and control the IP parameters. This menu is reached from the Main Menu through the Manage UDP/IP Menu (see Figure 5.1) by selecting the Manage IP Parameters option. Figure 5.4 illustrates the Manage IP Parameters Menu.

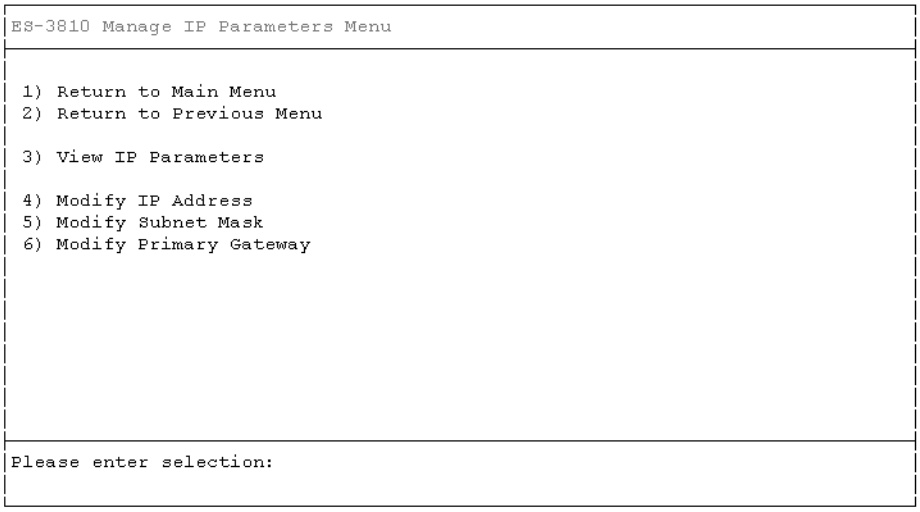


Figure 5.4 - Manage IP Parameters Menu

The items in the Manage IP Parameters Menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage UDP / IP Menu.
View IP Parameters	Displays the IP Parameters View screen.
Modify IP Address	Queries the user for a new IP address. The new IP address defaults to the current IP address if the user provides no input.
Modify Subnet Mask	Queries the user for a new subnet mask. The new subnet mask defaults to the class of the current IP address if the user provides no input.
Modify Primary Gateway	Queries the user for a new primary gateway. The new primary gateway defaults to 0.0.0.0 if the user provides no input.

5.1.3 Manage IP Routing Table Menu

This menu displays commands that provide access to managed objects that monitor and control the IP routing table. This menu is reached from the Main Menu through the Manage UDP / IP Menu (see Figure 5.1) by selecting the Manage IP Route Table option. Figure 5.5 illustrates the Manage IP Routing Table Menu.

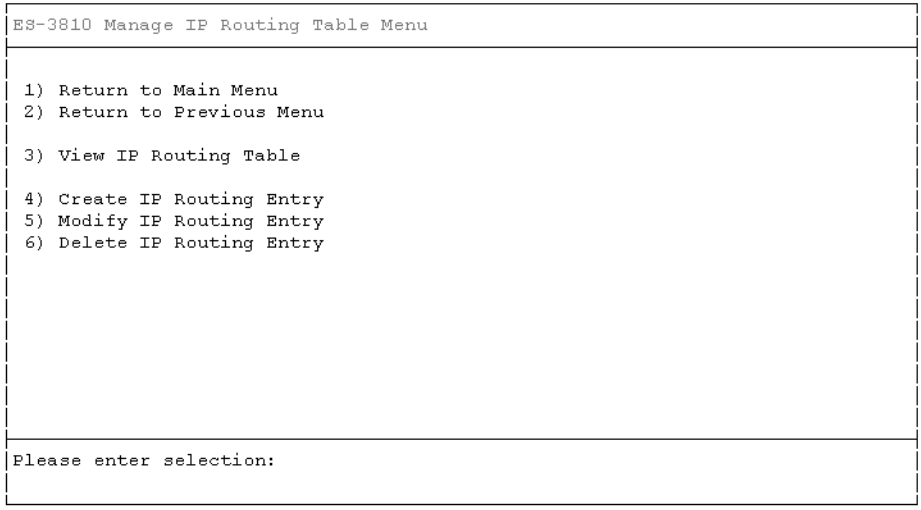


Figure 5.5 - Manage IP Routing Table Menu

The items in the Manage IP Routing Table Menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage UDP / IP Menu.
View IP Routing Table	Displays the IP Routing View screen.
Create IP Routing Entry	Queries the user for an IP address, a subnet mask, the next-hop address, and a simple routing metric. If the information provided by the user is valid, an entry does not already exist with the specified IP address, and the IP routing table is not full, then the management console adds an entry to the IP routing table.
Modify IP Routing Entry	Displays the IP routing entries and asks the user to select one. Next, the management console presents the user with the Modify IP Routing Entry Menu. If the specified entry does not exist in the IP routing table, then the management console displays an appropriate error message.

Delete IP Routing Entry Queries the user for an IP address. If the information provided by the user is valid, and the specified entry exists in the IP routing table, then the management console deletes the specific entry from the IP routing table. The management console confirms the action. If the specified entry does not exist in the IP routing table, then the management console displays an appropriate error message.

5.1.3.1 IP Routing Table View

This menu is reached from the Manage UDP / IP Menu (see Figure 5.1), then through the Manage IP Routing Table Menu (see Figure 5.5) by selecting the View IP Routing Table option. Figure 5.6 illustrates the IP Routing Table View screen.

IP Routing Table View 0 00:14:58.99

IP Address	Network Mask	Gateway	Metric	Fixed	Creator
123.234.12.34	255.255.255.255	Direct	0	Yes	Operational SW
123.234.12.0	255.255.255.0	Direct	0	Yes	Operational SW
Default	255.0.0.0	100.200.210.220	0	Yes	Operational SW

Figure 5.6 - IP Routing Table View

5.1.3.2 Modify IP Routing Entry Menu

This menu displays commands that provide write access to managed objects that define the specified IP routing entry. This menu is reached from the Manage UDP / IP Menu (see Figure 5.1) through the Manage IP Routing Table Menu (see Figure 5.5) by selecting the Modify IP Routing Entry option. Figure 5.7 illustrates the Modify IP Routing Entry Menu.

NOTE An IP route entry must be selected in the IP Route Entry Selection screen before this menu can be reached.

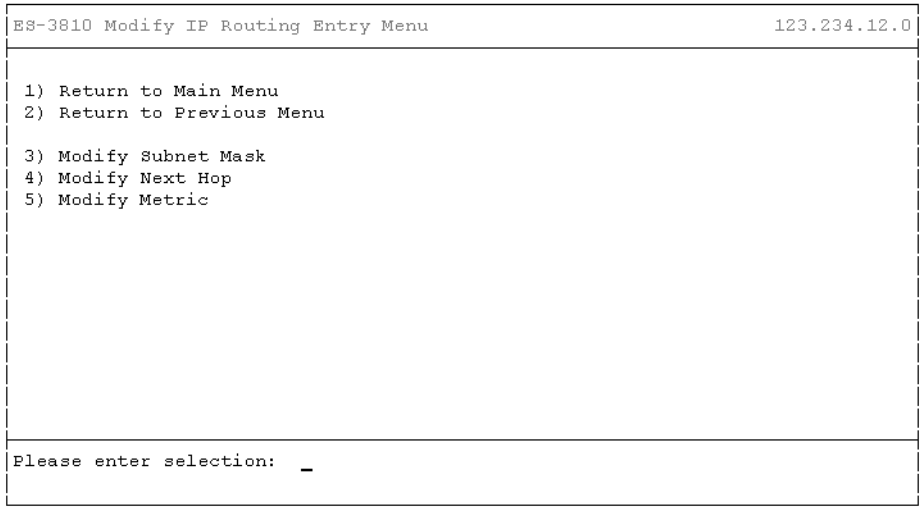


Figure 5.7 - Modify IP Routing Entry Menu

The items in the Modify IP Routing Entry Menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage IP Routing Table Menu.
Modify Subnet Mask	Queries the user for a new subnet mask for the specified IP routing entry. The new subnet mask defaults to the current subnet mask if the user provides no input.
Modify Next Hop	Queries the user for a new next-hop address for the specified IP routing entry. The new next-hop address defaults to the current next-hop address if the user provides no input.
Modify Metric	Queries the user for a new metric for the specified IP routing entry. The new metric defaults to the current metric if the user provides no input.

5.1.4 ICMP Counters

This view is reached from the Main Menu through the Manage UDP/IP Menu (see Figure 5.1) by selecting the View ICMP Counters option. Figure 5.8 illustrates the ICMP Counters screen where Inbound and Outbound ICMP counters can be viewed.


```
ES-3810 View ICMP Counters                                    27:13.69

              Inbound                          Outbound
Total Messages                    0 Total Messages                    0
Total Errors                      0 Total Errors                      0
Destination Unreachable Msgs      0 Destination Unreachable Msgs      0
Time Exceeded Messages            0 Time Exceeded Messages            0
Parameter Problem Msgs            0 Parameter Problem Msgs            0
Source Quench Messages            0 Source Quench Messages            0
Redirect Messages                 0 Redirect Messages                 0
Echo Requests                     0 Echo Requests                     0
Echo Replies                      0 Echo Replies                      0
Timestamp Requests                0 Timestamp Requests                0
Timestamp Replies                 0 Timestamp Replies                 0
Address Mask Requests             0 Address Mask Requests             0
Address Mask Replies              0 Address Mask Replies              0

=> _
Commands:  +, -, Freeze, Unfreeze, Quit
```

Figure 5.8 - View ICMP Counters

5.1.5 IP Counters

This view is reached from the Main Menu through the Manage UDP / IP Menu (see Figure 5.1) by selecting the View IP Counters option. Figure 5.9 illustrates the IP Counters screen.

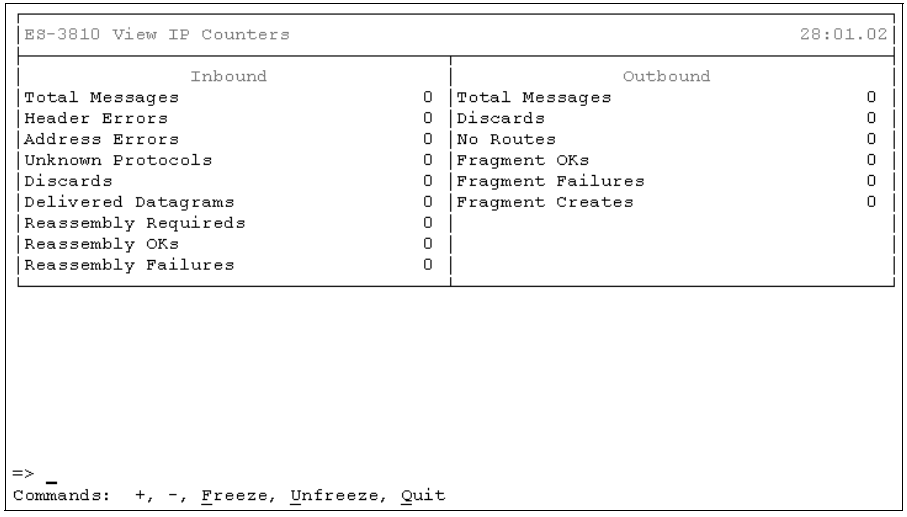


Figure 5.9 - View IP Counters

5.1.6 UDP Counters

This view is reached from the Main Menu through the Manage UDP / IP Menu (see Figure 5.1) by selecting the View UDP Counters option. Figure 5.10 illustrates the UDP Counters screen.

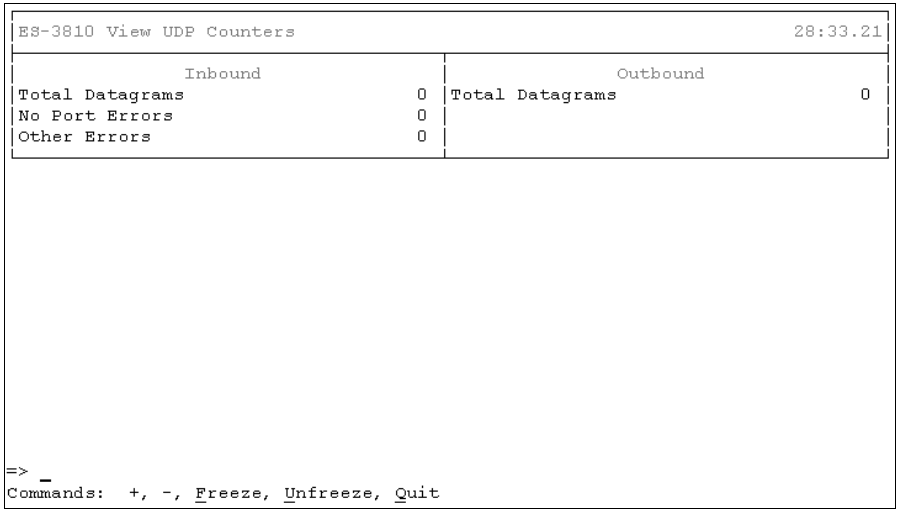


Figure 5.10 - UDP Counters View

5.1.7 Ping

This view is reached from the Main Menu through the Manage UDP / IP Menu (see Figure 5.1) by selecting the Ping option. Figure 5.11 illustrates the Ping screen.

```
IP Destination [147.128.20.253]: 147.128.20.253
Data Length [64]: 64


Hit RETURN to stop PING at any time.


Ping Statistics

Requests Sent    : 2
Replies Received : 0
Packet Loss      : 100%
Minimum RTT      : not applicable
Maximum RTT      : not applicable
Average RTT      : not applicable


Hit RETURN to continue:
```

CHAPTER 6 SNMP Management

This chapter describes the menus used to access and configure managed objects that monitor and control the SNMP-based management agent.

6.1 Manage SNMP Menu

This menu is reached directly from the Main Menu through the Manage SNMP option. Figure 6.1 illustrates the Manage SNMP Menu.

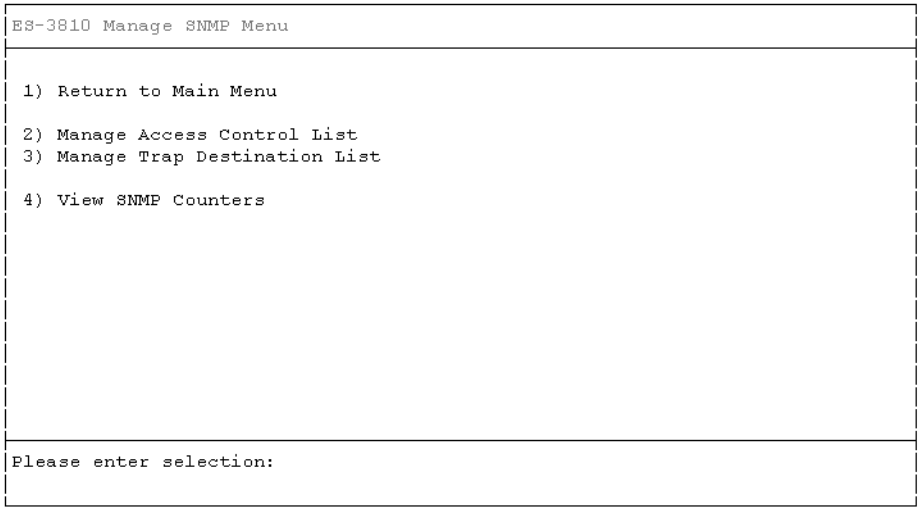


Figure 6.1 - Manage SNMP Menu

The items in the previous menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Manage Access Control List	Displays the Manage Access Control List Menu.
Manage Trap Destination List	Displays the Manage Trap Destination List Menu.
View SNMP Counters	Displays the SNMP Counters screen.

6.1.1 Manage Access Control List Menu

This menu displays commands that provide write access to managed objects that define the specified IP routing entry. These commands provide access to managed objects that monitor and control the access control list used by the SNMP-based agent for the purpose of authentication. The logon process also uses the access control list.

Entries can be added, deleted, and modified from the Access Control List. Communities and clients can be added to this list to give certain privileges to certain users. For example, you can add the community “Marketing,” and provide read-only privileges. The username for a community is the community name.

This menu is reached from the Main Menu through the Manage SNMP Menu, then through the Manage Access Control List option. Figure 6.2 illustrates the Manage Access Control List Menu.

```
ES-3810 Manage Access Control List Menu

 1) Return to Main Menu
 2) Return to Previous Menu

 3) View Access Control List

 4) Add Entry
 5) Delete Entry
 6) Modify Entry

 7) Add Client
 8) Delete Client
 9) Modify Client

Please enter selection:  _
```

Figure 6.2 - Manage Access Control List Menu

The items in the previous menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage SNMP Menu.
View Access Control List	Displays the Access Control List screen, listing communities and their IP addresses and clients.

Add Entry Queries the user for a new community name and whether or not that community has write privileges.

Delete Entry Displays a list of existing entries (communities) in the access control list and asks the user to select the entry to be deleted.

Modify Entry Displays a list of existing entries (communities) in the access control list and asks the user to select the entry to be modified, the new name for the entry, and the read-write privileges of the entry.

Add Client Displays a list of existing entries (communities) in the access control list and asks the user to select the entry to which a client is to be added. Next, the user is asked for the IP address, IP address mask, whether the client is to have write access (if the community to which it belongs has write access), and whether the client is to have read access.

A client cannot have more privileges than the community to which it belongs (i.e., a client in a "read-only" community cannot have write access).

Delete Client Displays a list of existing entries (communities) in the access control list and asks the user to select the entry from which a client is to be deleted. Next, a list of clients in the selected community is displayed, and the user is asked which client from the list is to be deleted.

Modify Client Displays a list of existing entries (communities) in the access control list and asks the user to select the entry containing the client to be modified. Next, a list of clients in the selected community is displayed, and the user is asked which client from the list is to be modified. The user must supply the client's new IP address, IP address mask, whether the client is to have write access (if the community to which it belongs has write access), and whether the client is to have read access.

6.1.1.1 Access Control List View and Community Selection

This view is reached from the Main Menu through the Manage SNMP Menu, then through the Manage Access Control List Menu, and finally through the View Access Control List option. Figure 6.3 illustrates the Access Control List View screen.

```
ES-3810 Access Control List

Id | Community                                          | Rights | Client List
---+----------------------------------------------------+--------+------------
 1 | public                                             |   R    |     No
 2 | private                                            |   RW   |     No
 3 | marketing                                          |   R    |     Yes
 4 | sales                                              |   R    |     No

Hit <enter> to return to the previous menu or
type a community id to view its client list: 3_
```

Figure 6.3 - Access Control List View

6.1.1.2 Client List View

This view is reached from the Main Menu through the Manage SNMP Menu, then through the Manage Access Control List Menu, and finally through the View Access Control List option by typing in a community ID from the Access Control List (see Figure 6.3). Figure 6.4 illustrates the Access Control List View screen.

```
ES-3810 Client List for Community "marketing"                  0 05:13:03.18

 Id | Client Address                | Client Mask                   | Rights
----+-------------------------------+-------------------------------+--------
 1  | 147.128.20.252                | 255.255.255.255               |   RW
 2  | 147.128.20.253                | 255.255.255.255               |   R
 3  | 147.128.20.254                | 255.255.255.255               |   R

 Hit <Enter> to continue.
```

Figure 6.4 - Client List View

6.1.2 Manage Trap Destination List Menu

This menu displays commands that provide access to managed objects that monitor and control the trap destination list used by the SNMP-based agent to determine where to send traps. This menu is reached from the Main Menu through the Manage SNMP Menu. Figure 6.5 illustrates the Manage Trap Destination List Menu.

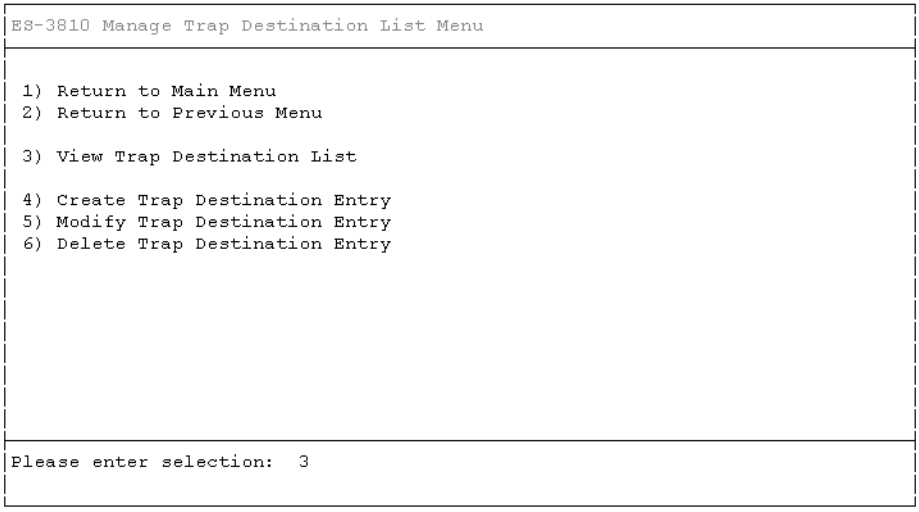


Figure 6.5 - Manage Trap Destination List Menu

The items in the previous menu have the following meanings:

Return to Main Menu	Returns to the Main Menu.
Return to Previous Menu	Returns to the Manage SNMP Menu.
View Trap Destination List	Displays the Trap Destination List View.

Create Trap Destination Entry — Queries the user for an IP address and a community name. If the information provided by the user is valid, and an entry matching the specified IP address does not already exist in the trap destination list, and the trap destination list is not full, then the management console adds the entry to the trap destination list. If the management console could not add the entry to the trap destination list, then the management console displays an appropriate error message in the error message component of the Manage Trap Destination List Menu. Note that trap destination entries are persistent.

Modify Trap Destination Entry — Displays the Trap Destination Selection screen and then queries the user for a new community. The new community defaults to the current community if the user provides no input.

Delete Trap Destination Entry — Displays the Trap Destination List View screen and then asks the user to confirm the selection before deleting the entry.

6.1.2.1 View Trap Destination List

This view is reached from the Main Menu through the Manage SNMP Menu, and then through the Manage Trap Destination List Menu by choosing the View Trap Destination List option. Figure 6.6 illustrates the Trap Destination List View screen.

```
ES-3810 Trap Destination List                                  0 05:27:02.20

 Id  | Client          |  Community

 1   | 12.34.23.45     | sales
 2   | 34.56.123.12    | marketing
 3   | 123.234.12.34   | public
 4   | 255.0.0.0       | private

Hit <Enter> to continue.
```

Figure 6.6 - View Trap Destination List

6.1.3 SNMP Counters

This view is reached from the Main Menu through the Manage SNMP Menu, using the View SNMP Counters option. Figure 6.7 illustrates the View SNMP Counters screen.

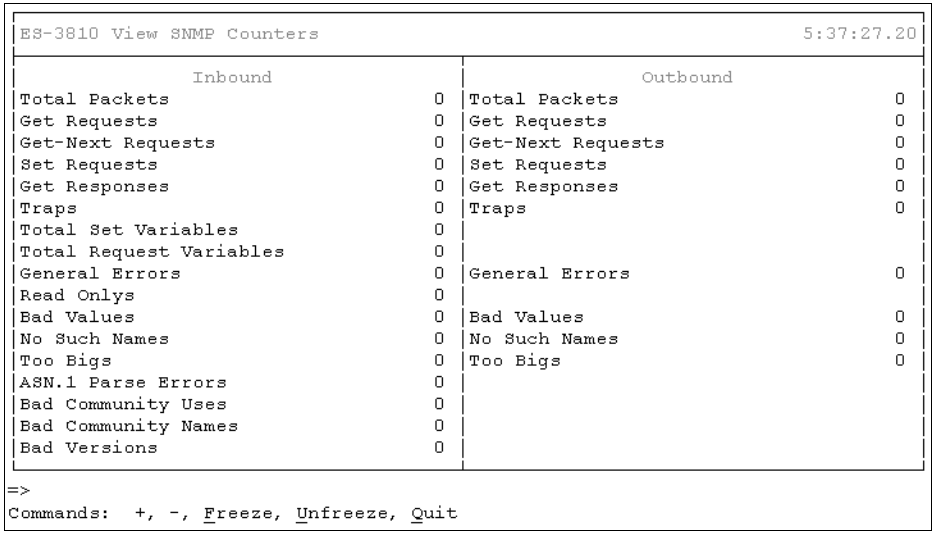


Figure 6.7 - View SNMP Counters

CHAPTER 7 Spanning Tree Management

This section provides an overview of Spanning Tree bridging and details the menus used to manage and configure it on the ES-3810.

7.1 Overview

A bridge accepts packets of data passing through a network and decides whether to forward each packet based on the information it contains. Bridges operate at the physical and data link layers of the Open Systems Interconnection (OSI) model. The physical layer provides the physical connection to the transmission medium, and the data link layer provides reliable transmission. Specifically, the data link layer is made up of two distinct tasks, Logical Link Control (LLC) and Media Access Control (MAC) (see Figure 7.1).

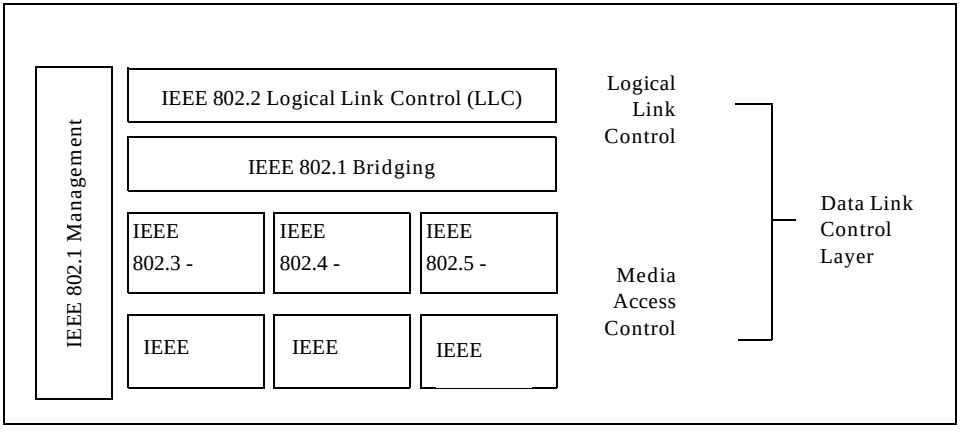


Figure 7.1 - Overview of IEEE Protocols

The LLC controls the logical link (i.e., it serves to open, maintain, and terminate links). The LLC depends upon the physical layers to perform its tasks.

The MAC controls access to the physical media, acting independently of the physical layer and providing an interface to the upper layers of the network model. IEEE 802.3 and Ethernet use the same MAC layer, allowing both types of packets to coexist on the same cable. In this way, the same bridge can forward both Ethernet and IEEE 802.3 packets.

Bridging allows any IEEE 802-compliant station to communicate with remote, bridged stations as if they were local. Although bridged networks remain physically separate, they appear as one network to other devices.

Bridges forward packets between networks and can pass data using any protocol compatible with the media. Bridges receive all packets from a LAN and examine each one to determine its destination. If the packet is destined for a station on the physical cable from which it was received, the bridge does not forward the packet. If the destination is unknown, the packet is forwarded to all ports except the one on which it was received.

Because bridges examine each packet, and because each packet contains a source address, bridges can easily learn the locations of stations on the network. However, if an address is unknown, flooding can result in endless loops on the network, since all bridges that do not know the address will flood the packet looking for the address. To circumvent this, a tree-type algorithm is implemented that prevents loops and forces the packets into logical routes. This algorithm, called the Spanning Tree Algorithm (STA), allows only one route between any two physical cables or networks.

Spanning tree bridges are based upon a root bridge which exchanges topology information with designated bridges to maintain the configuration. The root and designated bridges notify all other bridges in the network when topology changes are required, thereby preventing loops and reducing the risk of link failure.

7.1.1 Spanning Tree on the ES-3810

The ES-3810 supports up to 16 Spanning Tree instances, or bridges. Each bridge must be configured on a per-port, per-VLAN basis. All ports of a VLAN must be associated with the same Spanning Tree, including the ports of the associated ELAN (denoted as L1, L2, etc.).

More than one VLAN can be associated with a bridge.

Each bridge, internally numbered from 0 to 15, can be named to allow easier identification. At startup, a default bridge (STP 0) is configured. This default instance is named `DefaultSpanningTree`.

All VLANS and all ports belong to STP 0 by default, and all ports will be initialized with Spanning Tree switched-off. Spanning Tree must be manually activated on desired ports (see the remainder of this chapter for more information on configuring Spanning Tree on the ES-3810).

7.2 Manage Spanning Tree Menu

The Manage Spanning Tree Menu is available from the Main Menu of the ES-3810 console interface by selecting the Manage Spanning Tree option. Figure 7.2 illustrates the Manage Spanning Tree Menu.

```
ES-3810 Manage Spanning Tree Menu                          DefaultSpanningTree

 1) Return to Main Menu
 2) Select Spanning Tree Instance

 3) Display Spanning Tree Bridge Information

 4) Create Spanning Tree Instance
 5) Modify Spanning Tree Bridge Config
 6) Delete Spanning Tree Instance

 7) Display Spanning Tree Port Status

 8) Switch STP ON  on Ports
 9) Switch STP OFF on Ports
10) Manage Spanning Tree Port Configuration


Please enter selection:  _
```

Figure 7.2 - Manage Spanning Tree Menu

7.2.1 Selecting a Spanning Tree Instance

From the Manage Spanning Tree Menu (see Figure 7.2) select the Select Spanning Tree Instance option. When the Select Spanning Tree screen appears, type the number corresponding to the desired Spanning Tree instance and press <ENTER> (see Figure 7.3).

```
ES-3810 Select Spanning Tree                              DefaultSpanningTree

Number | Name
-------+-------------------------------------------------------------------
   1   | DefaultSpanningTree
   2   | Spanning Tree 1
   3   | Spanning Tree 2
   4   | Spanning Tree 3
-------+-------------------------------------------------------------------
Please enter selection (by Number):
```

Figure 7.3 - Select Spanning Tree Menu

7.2.2 Displaying Spanning Tree Bridge Information

After selecting a Spanning Tree instance, you will be returned to the Manage Spanning Tree Menu (see Figure 7.2). To display the bridge information of the selected Spanning Tree instance, select the Display Spanning Tree Bridge Information option. The screens shown in Figure 7.4 and Figure 7.5 are displayed.

```
Spanning Tree Management              Bridge Information       0 00:09:34.23

STP Name : Spanning Tree 1            STP Number      1

Root Port Number          0 ()        Desig Root Pr         32768

Root Cost                 0           Desig Root Ad         00-A0-36-00-05-61

Topology Changes 0                    Bridge Priority       32768

Hold Time             1 secs          Bridge Address        00-A0-36-00-05-61

Max Age               20 secs         Bridge Max Age        20 secs

Hello Time            2 secs          Bridge Hello Time     2 secs

Forward Delay         15 secs         Bridge Forward Delay  15 secs


Enter any key to continue
```

Figure 7.4 - Bridge Information Display (Part 1)

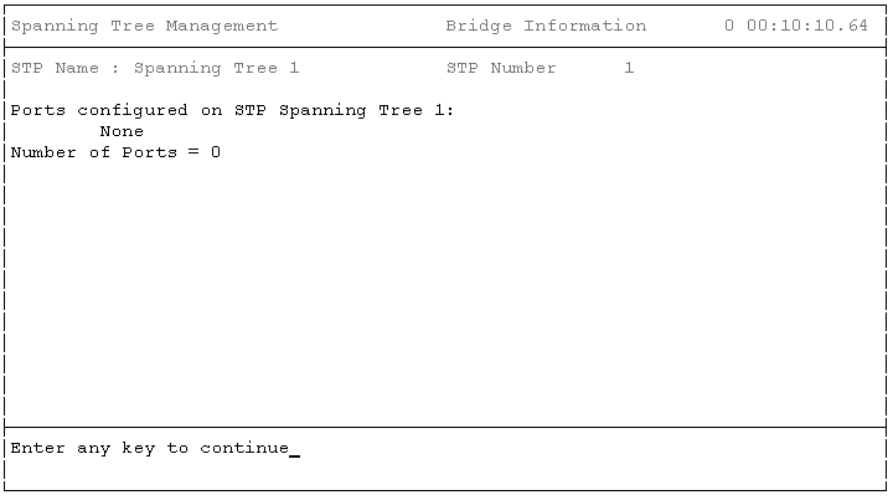


Figure 7.5 - Bridge Information Display (Part 2)

The parameters displayed in Figure 7.4 and Figure 7.5 have the following meanings:

STP Name — Indicates the name of the selected bridge. A bridge's name can be assigned or changed by the user. The default bridge name is `DefaultSpanningTree`.

STP Number — Indicates the number, from 0 to 15, of the selected bridge. `STP Number` is the internal system identifier of each bridge.

Root Port Number — Indicates the port on the selected bridge that is closest to the Root Bridge, determined by path cost.

Desig Root Pr — Indicates the priority of the root bridge, between 0 and 65,535.

Root Cost — Indicates the sum of the path costs from the selected bridge to the root.

Desig Root Ad — Indicates the MAC address of the root bridge.

Topology Changes — Indicates the number of times the topology of the selected bridge has changed.

Bridge Priority — Indicates the priority of the selected bridge.

Hold Time — Indicates the hold time, which is a constant value of one second.

Bridge Address	Indicates the MAC address of the selected bridge.
Max Age	Indicates the maximum amount of time that the selected bridge will wait to hear Hello Bridge Protocol Data Units (BPDUs) from the root bridge. If the selected bridge does not receive BPDUs from the root bridge within this interval, it assumes that the network has changed and recalculates the spanning tree topology.
Bridge Max Age	Indicates the Max Age of the selected bridge.
Hello Time	Indicates the interval between BPDUs.
Bridge Hello Time	Indicates the Hello Time for the selected bridge.
Forward Delay	Indicates the amount of time that will be spent listening for topology changes after a bridging interface is configured and before forwarding begins.
Bridge Forward Delay	Indicates the Forward Delay for the selected bridge.

7.2.3 Creating a Spanning Tree Instance

To create a new Spanning Tree instance, select the Create Spanning Tree option from the Manage Spanning Tree Menu (see Figure 7.2). The Create Spanning Tree screen is displayed (see Figure 7.6).

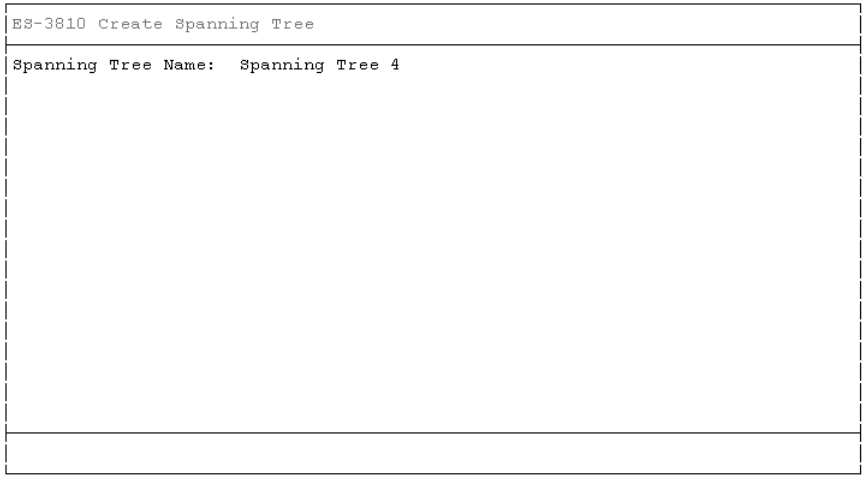


Figure 7.6 - Create Spanning Tree Menu (part 1)

Type the name of the new Spanning Tree and press <ENTER>. Next, select a VLAN to include in the new spanning tree (see Figure 7.7). If you wish to include ports from another VLAN, enter **y** at the `Add More Ports from Vlans [No]?` prompt (see Figure 7.7).

```
ES-3810 Create Spanning Tree                          STP 7 (Spanning Tree 4)

 Ports configured on STP Spanning Tree 4:
        None
 Select Vlan to include in this Spanning Tree :

 1. default




Enter Vlan Number :1


  Add More Ports from Vlans [No]?  n
```

Figure 7.7 - Create Spanning Tree Menu (part 2)

7.2.4 Modifying Spanning Tree Bridge Information

To modify the bridge information of the selected Spanning Tree instance, select the Modify Spanning Tree Bridge Configuration option from the Manage Spanning Tree Menu (see Figure 7.2). The Modify Spanning Tree Bridge Configuration Menu is displayed (see Figure 7.8).

```
ES-3810 Modify Spanning Tree Bridge Config Menu            DefaultSpanningTree

 1) Return to Main Menu
 2) Return to Previous Menu
 3) Associate VLAN to STP Instance
 4) Modify STP Bridge Priority
 5) Modify STP Bridge MaxAge
 6) Modify STP Bridge Hello Time
 7) Modify STP Bridge Forward Delay

Please enter selection:
```

Figure 7.8 - Modify Spanning Tree Bridge Configuration Menu

7.2.4.1 Associating a VLAN to a Spanning Tree Instance

To associate a VLAN to the selected Spanning Tree instance, select the Associate VLAN to STP Instance option from the Modify Spanning Tree Bridge Configuration Menu. The Associate VLANs to Spanning Tree screen is displayed (see Figure 7.9). Type the number corresponding to the desired VLAN and press <ENTER>.

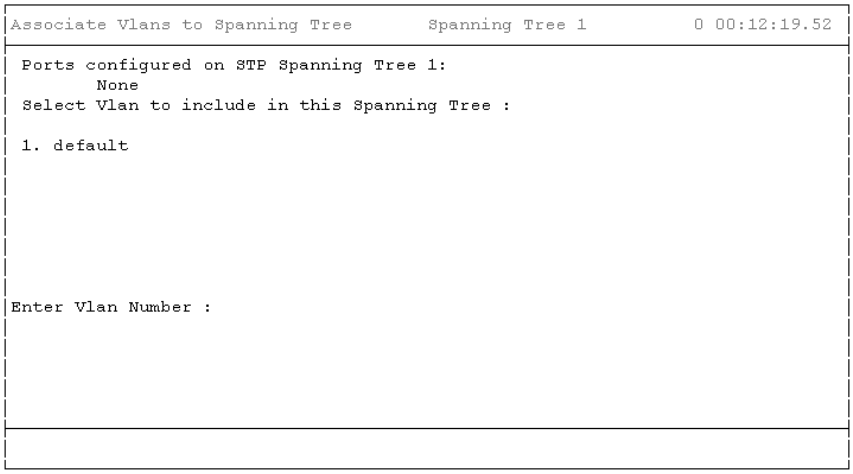


Figure 7.9 - Associate VLANS to Spanning Tree Menu

7.2.4.2 Modifying Spanning Tree Bridge Priority

To modify the Spanning Tree bridge priority of the selected Spanning Tree instance, select the Modify STP Bridge Priority option from the Modify Spanning Tree Bridge Configuration Menu. The Modify STP Bridge Priority screen is displayed (see Figure 7.10). Type the value of the new bridge priority and press <ENTER>.

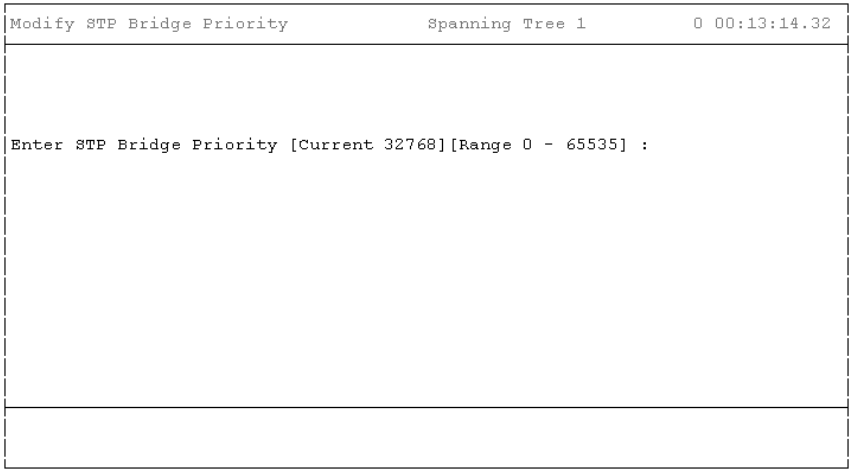


Figure 7.10 - Modify STP Bridge Priority Menu

7.2.4.3 Modifying Spanning Tree Bridge Maximum Age

To modify the Spanning Tree bridge maximum age of the selected Spanning Tree instance, select the Modify STP Bridge MaxAge option from the Modify Spanning Tree Bridge Configuration Menu. The Modify STP Bridge MaxAge screen is displayed (see Figure 7.11). Type the value of the new maximum age and press <ENTER>.

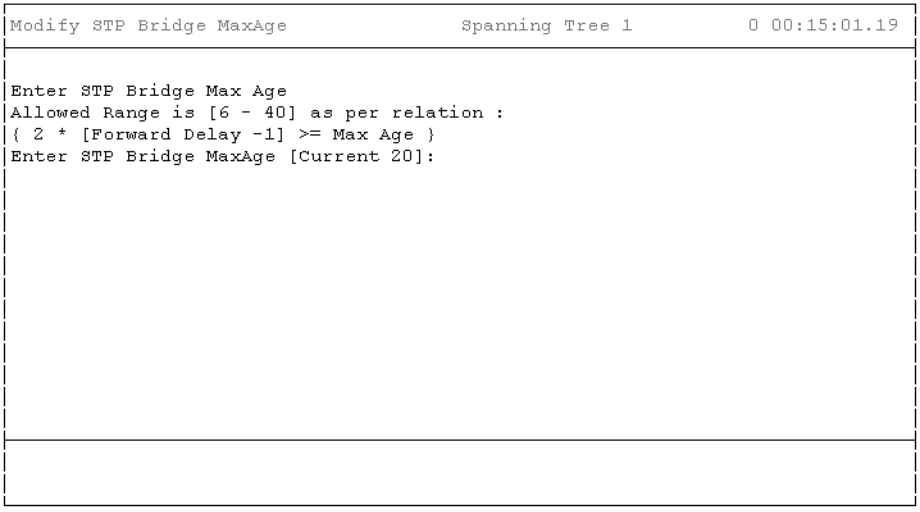


Figure 7.11 - Modify STP Bridge MaxAge Menu

7.2.4.4 Modifying Spanning Tree Bridge Hello Time

To modify the Spanning Tree bridge hello time of the selected Spanning Tree instance, select the Modify STP Bridge Hello Time option from the Modify Spanning Tree Bridge Configuration Menu. The Modify STP Bridge Hello Time screen is displayed (see Figure 7.12). Type the value of the new hello time and press <ENTER>.

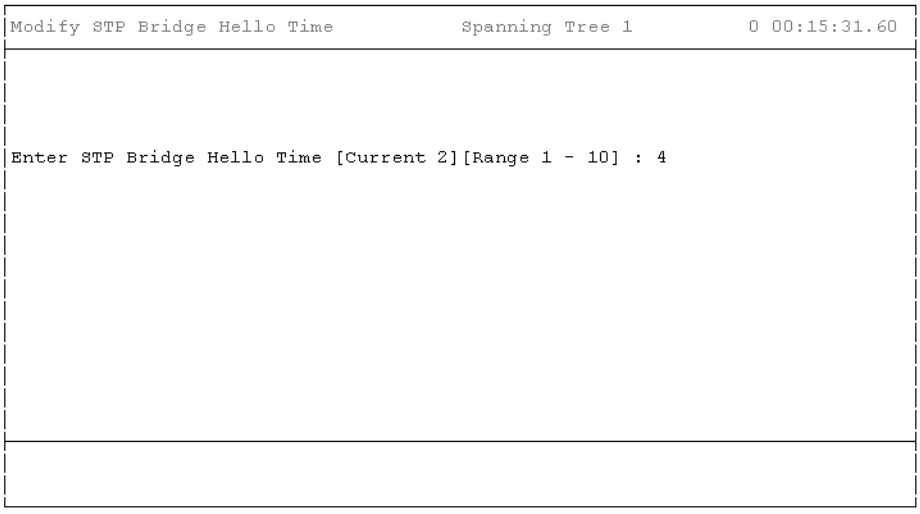


Figure 7.12 - Modify STP Bridge Hello Time Menu

7.2.4.5 Modifying Spanning Tree Bridge Forward Delay

To modify the Spanning Tree bridge forward delay of the selected Spanning Tree instance, select the Modify STP Bridge Forward Delay option from the Modify Spanning Tree Bridge Configuration menu. The Modify STP Bridge Forward Delay screen is displayed (see Figure 7.13). Type the value of the new forward delay and press <ENTER>.

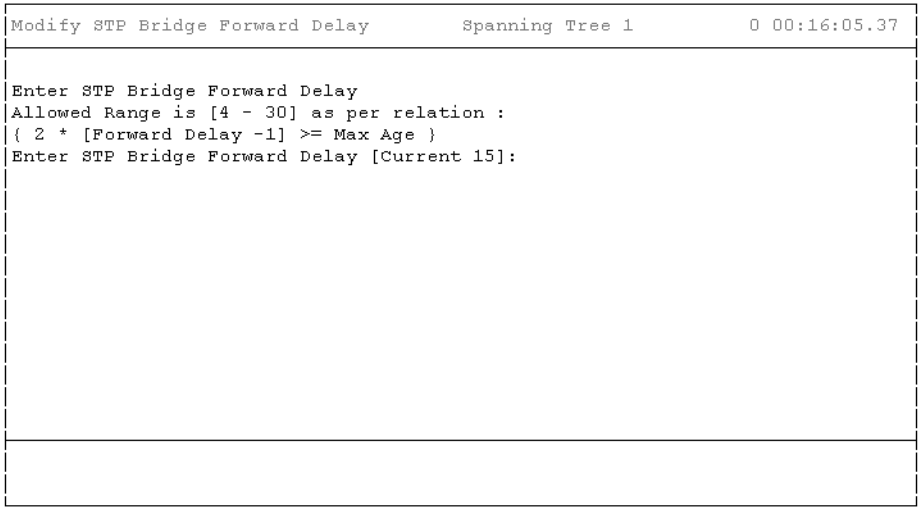


Figure 7.13 - Modify STP Bridge Forward Delay Menu

7.2.5 Deleting a Spanning Tree Instance

To delete a Spanning Tree instance, select the Delete Spanning Tree Instance from the Manage Spanning Tree Menu (see Figure 7.2). When the Delete Spanning Tree screen appears, type the number corresponding to the Spanning Tree instance to be deleted and press <ENTER> (see Figure 7.14).

```
ES-3810 Delete Spanning Tree                                Spanning Tree 1

Number | Name
-------+-------------------------------------------------------------------
   1   | DefaultSpanningTree
   2   | Spanning Tree 1
   3   | Spanning Tree 2
   4   | Spanning Tree 3
   5   | Spanning Tree 4

Please enter selection (by Number):
```

Figure 7.14 - Delete Spanning Tree Menu

7.2.6 Displaying Spanning Tree Port Status

To display all the ports of the ES-3810, the Spanning Tree instance to which they belong, and the status of each port, select the Display Spanning Tree Port Status option from the Manage Spanning Tree Menu (see Figure 7.2). When the View STP Port Status Display is shown, press <ENTER> to scroll through the listed ports (see Figure 7.15).

```
ES-3810 View STP Port Status                                  Spanning Tree 1

   1. DefaultSpanningTree            B1                  STP Off
   2. DefaultSpanningTree            B2                  STP Off
   3. DefaultSpanningTree            B3                  STP Off
   4. DefaultSpanningTree            B4                  STP Off
   5. DefaultSpanningTree            B5                  STP Off
   6. DefaultSpanningTree            B6                  STP Off
   7. DefaultSpanningTree            B7                  STP Off
   8. DefaultSpanningTree            B8                  STP Off
   9. DefaultSpanningTree            C1                  STP Off
  10. DefaultSpanningTree            C2                  STP Off
  11. DefaultSpanningTree            C3                  STP Off
  12. DefaultSpanningTree            C4                  STP Off
  13. DefaultSpanningTree            C5                  STP Off
  14. DefaultSpanningTree            C6                  STP Off
  15. DefaultSpanningTree            C7                  STP Off
  16. DefaultSpanningTree            C8                  STP Off
  17. DefaultSpanningTree            C9                  STP Off

Hit <ENTER> to View Remaining Ports
```

Figure 7.15 - View STP Port Status Display

7.2.7 Switching-on STP on Ports

To switch-on Spanning Tree on an individual port or groups of ports, select the Switch STP ON on Ports option from the Manage Spanning Tree Menu (see Figure 7.2). When the Switch STP ON screen appears, type the port(s) on which you wish to switch-on Spanning Tree and press <ENTER> (see Figure 7.16).

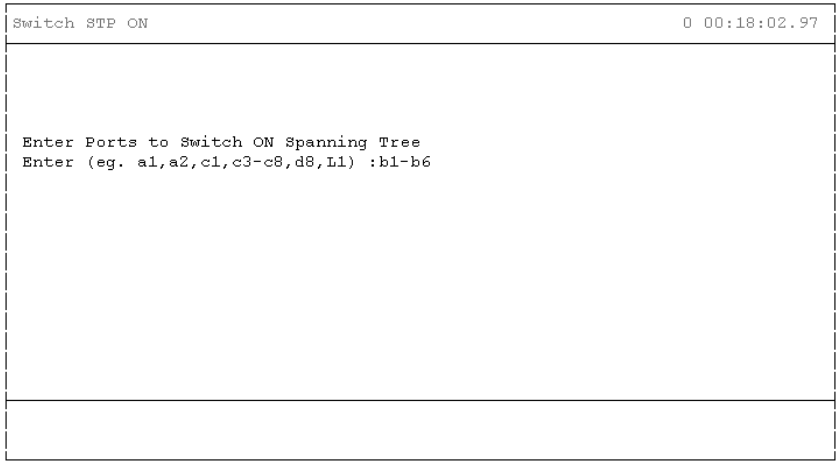


Figure 7.16 - Switch STP ON Menu

7.2.8 Switching-off STP on Ports

To switch-off Spanning Tree on a port or groups of ports, select the Switch STP OFF on Ports option from the Manage Spanning Tree Menu (see Figure 7.2). When the Switch STP OFF screen appears, type the port(s) on which you wish to switch-off Spanning Tree and press <ENTER> (see Figure 7.17).

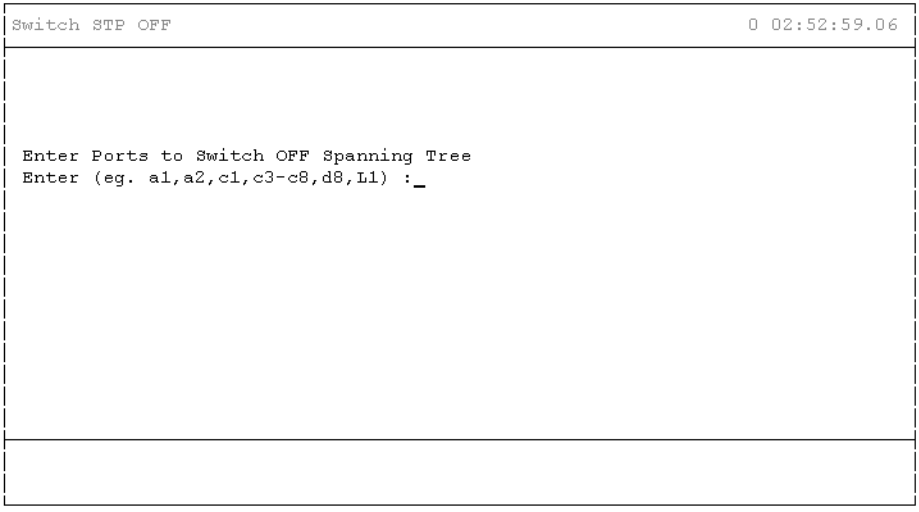


Figure 7.17 - Switch STP OFF Menu

7.2.9 Managing Spanning Tree Port Configuration

To manage Spanning Tree on a port, select the Manage Spanning Tree Port Configuration option from the Manage Spanning Tree Menu (see Figure 7.2). The Modify Spanning Tree Port Configuration Menu appears (see Figure 7.18).

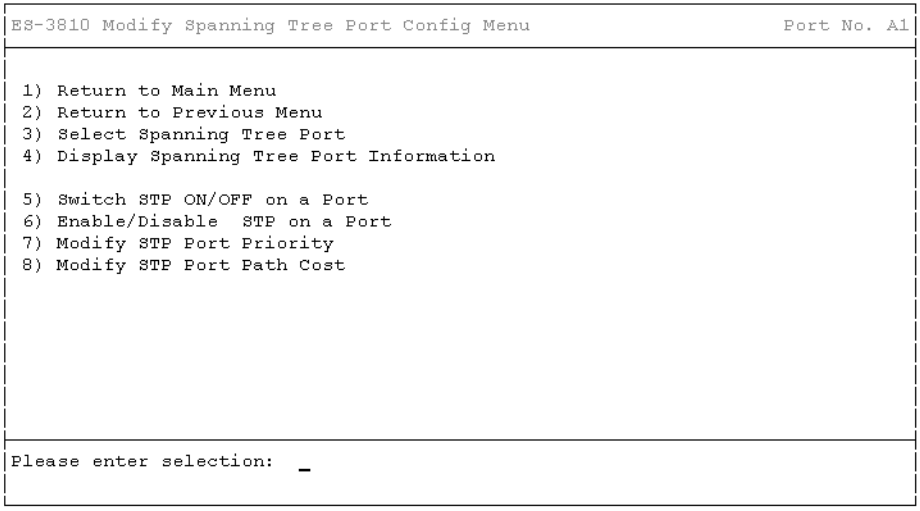


Figure 7.18 - Modify Spanning Tree Port Configuration Menu

7.2.9.1 Selecting a Spanning Tree Port

To manage Spanning Tree on an individual port, select the Select Spanning Tree Port option from the Modify Spanning Tree Port Configuration Menu (see Figure 7.18). When the Select Spanning Tree Port screen appears, enter the desired port number and press <ENTER> (see Figure 7.19).

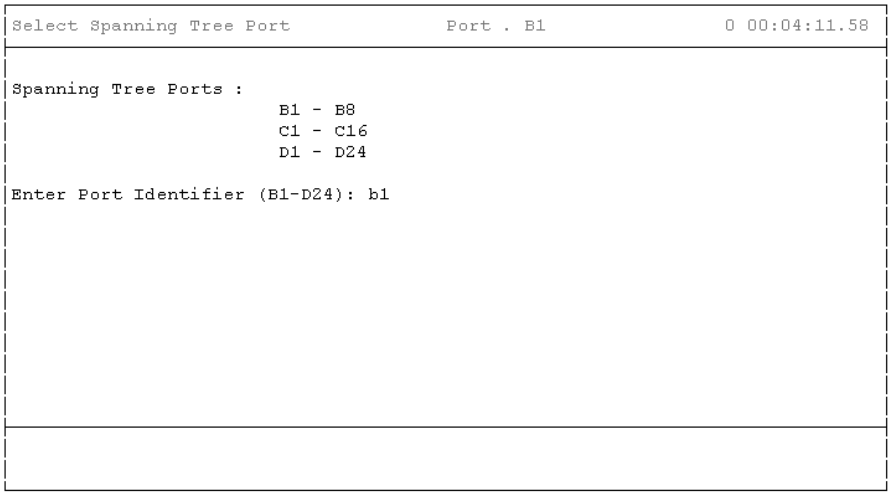


Figure 7.19 - Select Spanning Tree Port Menu

7.2.9.2 Displaying Spanning Tree Port Information

To display information for the selected port, select the Display Spanning Tree Port Information option from the Modify Spanning Tree Port Configuration Menu (see Figure 7.18). The Spanning Tree Management Display is shown (see Figure 7.20).

```
Spanning Tree Management                Port Information          0 00:04:43.10

STP Information for Port B1             Desig Root Pr         0
Port Priority             128           Desig Root Ad         00-00-00-00-00-00
Port Id                   1             Desig Cost            0
Port State                STP Off       Desig Bridge Pr     0
Port Path Cost            10            Desig Bridge Ad     00-00-00-00-00-00
Designated Port Priority  0             Designated Port Id    0
Spanning Tree Instance = 0              STP Name : DefaultSpanningTree

Enter any key to continue
```

Figure 7.20 - Spanning Tree Port Information Menu

7.2.9.3 Toggling STP on a Port

To switch STP on or off on the selected port, select the Switch STP ON / OFF on a Port option from the Modify Spanning Tree Port Configuration Menu (see Figure 7.18). If Spanning Tree is currently set to ON on the port, you will be prompted to turn it OFF. If Spanning Tree is currently set to OFF, you will be prompted to turn it ON. Type **y** and press <ENTER> at the prompt to accept, or type **n** and press <ENTER> to leave the port unchanged (see Figure 7.21).

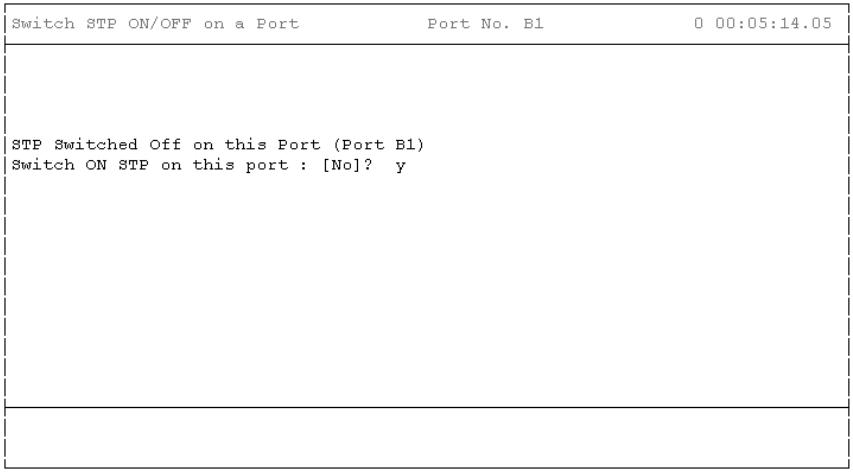


Figure 7.21 - Toggle STP on a Port Menu

7.2.9.4 Enabling/Disabling Traffic Forwarding on a Port

To enable or disable traffic forwarding on the selected port, select the Enable / Disable STP on a Port option from the Modify Spanning Tree Port Configuration Menu (see Figure 7.18). If traffic forwarding is currently enabled on the port, you will be prompted to disable it. If traffic forwarding is currently disabled on the port, you will be prompted to enable it. Type **y** and press <ENTER> at the prompt to accept, or type **n** and press <ENTER> to leave the port unchanged (see Figure 7.22).

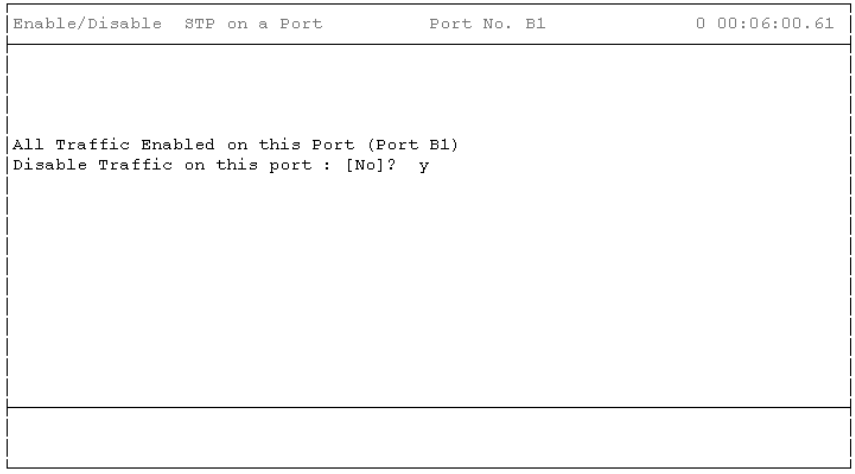


Figure 7.22 - Enable / Disable STP Menu

7.2.9.5 Modifying STP Port Priority

To modify a port's priority, select the Modify STP Port Priority option from the Modify Spanning Tree Port Configuration Menu (see Figure 7.18). When the Modify STP Port Priority screen appears, type a new port priority and press <ENTER> (see Figure 7.23).

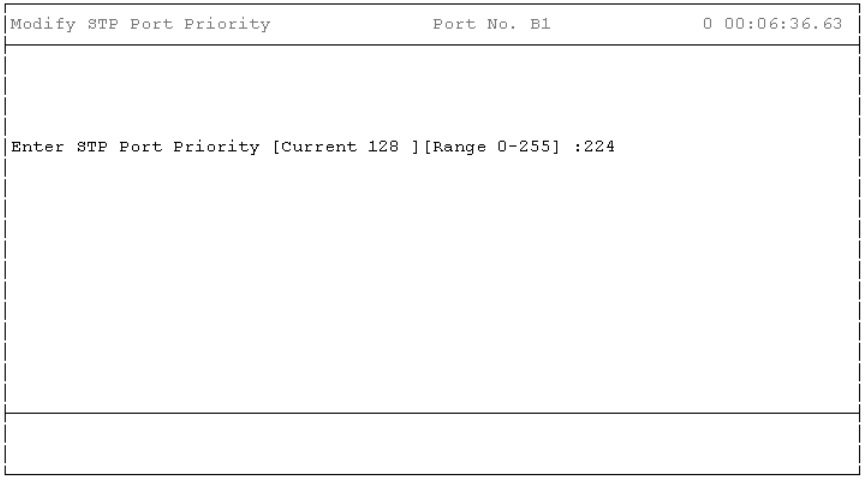


Figure 7.23 - Modify STP Port Priority Menu

7.2.9.6 Modifying STP Port Path Cost

To modify the path cost on a selected port, select the Modify STP Port Path Cost option from the Modify Spanning Tree Port Configuration Menu (see Figure 7.18). When the Modify STP Port Path Cost screen appears, type a new path cost and press <ENTER> (see Figure 7.24).

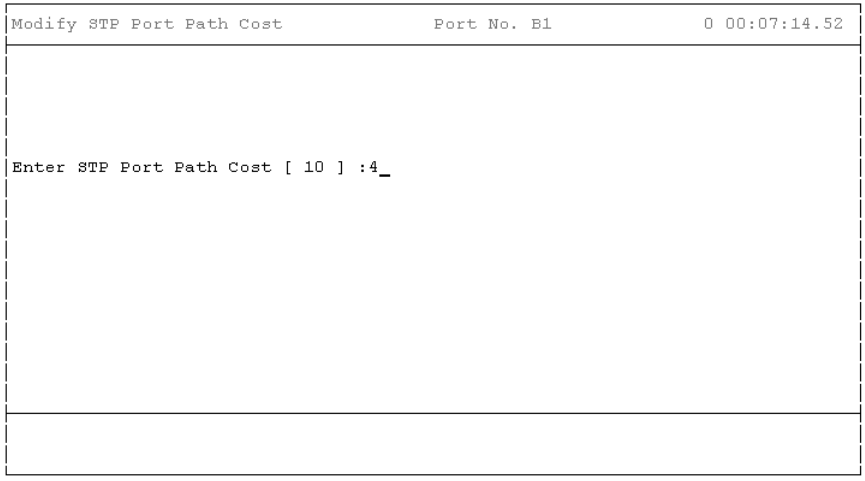


Figure 7.24 - Modify STP Port Path Cost Menu

CHAPTER 8 Telnet Management

8.1 Overview

The ES-3810 includes single-session Telnet support for providing remote access to the switch.

Telnet is single session **only** and causes the console to be redirected (i.e., only a telnet session or a local console session can be active at any one time, not both).

To configure Telnet on the ES-3810, log on via the management console and select the Manage Telnet option from the Main Menu. The Manage Telnet Menu is displayed, as shown in Figure 8.1.

```
ES-3810 Manage Telnet Menu

 1) Return to Main Menu

 2) View Telnet Parameters

 3) Enable/Disable Telnet
 4) Modify Telnet Timeout

 5) View TCP Connections

Please enter selection: _
```

Figure 8.1 - The Manage Telnet Menu

8.1.1 Viewing Telnet Parameters

To view the ES-3810's current Telnet configuration, select the View Telnet Parameters option from the Manage Telnet Menu (see Figure 8.1). The Telnet parameters are displayed as shown in Figure 8.2.

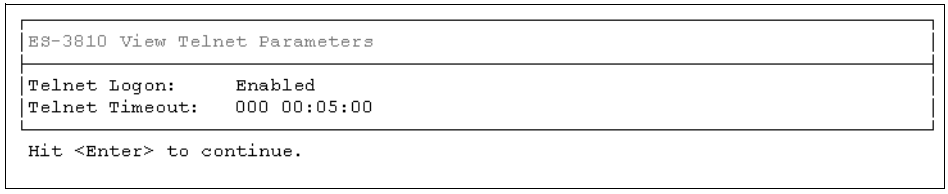


Figure 8.2 - View Telnet Parameters Display

The parameters displayed in this screen have the following meanings:

Telnet Logon — Indicates whether or not Telnet access to the ES-3810 is enabled. `Enabled` indicates that the ES-3810 can be reached via telnet (using the correct IP address). `Disabled` indicates that the ES-3810 can not be reached via Telnet.

Telnet Timeout — Indicates the current timeout setting for the ES-3810. The timeout parameter (entered in `days hours:minutes:seconds`) indicates the amount of "idle" time allowed before which the ES-3810 will terminate a Telnet session.

For example, if the timeout value is set to `000 00:05:00` (five minutes), a Telnet session to the ES-3810 will be terminated after five minutes of inactivity.

8.1.2 Enabling/Disabling Telnet

To enable or disable Telnet on the ES-3810, select the Enable / Disable Telnet option from the Manage Telnet Menu (see Figure 8.1). The selection must be confirmed (whether enabling or disabling Telnet), as shown in Figure 8.3.

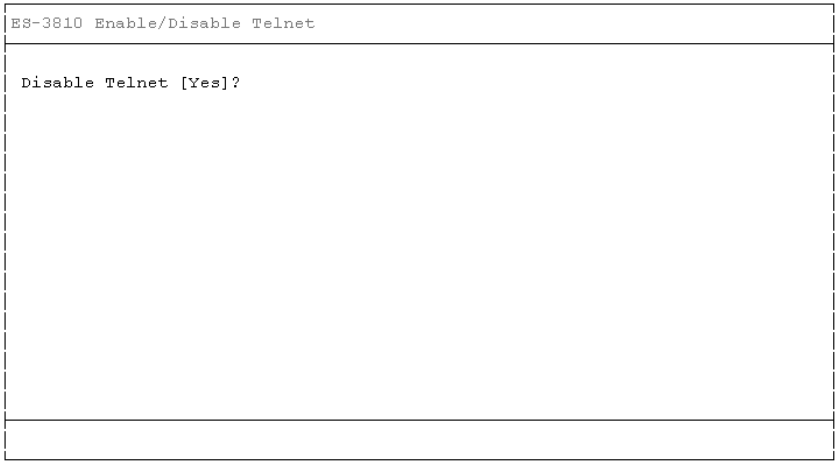


Figure 8.3 - Enable / Disable Telnet Confirmation Screen

If Telnet is disabled, the following message is displayed: `Enable Telnet [Yes]?`

1. To enable Telnet:
   - Type **y** and press <ENTER>, or simply press <ENTER>.
2. To leave Telnet disabled:
   - Type **n** and press <ENTER>.
   - Next, press <ENTER> again to return to the Manage Telnet Menu.

If Telnet is enabled, the following message is displayed: `Disable Telnet [Yes]?`

1. To disable Telnet:
   - Type **y** and press <ENTER>, or simply press <ENTER>.
2. To leave Telnet enabled:
   - Type **n** and press <ENTER>.
   - Next, press <ENTER> again to return to the Manage Telnet Menu.

8.1.3 Modifying the Timeout Value

To change or disable the Telnet timeout value on the ES-3810, select the Modify Telnet Timeout option from the Manage Telnet Menu (see Figure 8.1). The screen shown in Figure 8.4 is displayed.

```
ES-3810 Modify Telnet Timeout

Telnet Timeout [5:00]:  000 00:10:00_

Please enter a delta time value using the following format:

     [ddd hh:mm:]ss

  where ddd = days (<12)
        hh  = hours (<24)
        mm  = minutes (<60)
        ss  = seconds (<60)
 Delta time should be >= 10secs AND <= 1000000secs


  Enter a zero (0) value to disable the function.
```

Figure 8.4 - Timeout Modification Screen

To change the Telnet timeout value, enter the new value according to the key in the lower portion of the screen. For example, to change the value to 10 minutes, enter `000 00:10:00`. Ten minutes can also be entered as `10:00`, or as `600` (seconds).

To return to the Manage Telnet Menu without modifying the timeout value, press <ENTER> before entering anything else.

To disable the timeout feature altogether, enter **0** as the timeout value.

8.1.4 Viewing TCP Connections

To view the TCP connections on the ES-3810, select the View TCP Connections option from the Manage Telnet Menu (see Figure 8.1). The screen shown in Figure 8.5 is displayed.

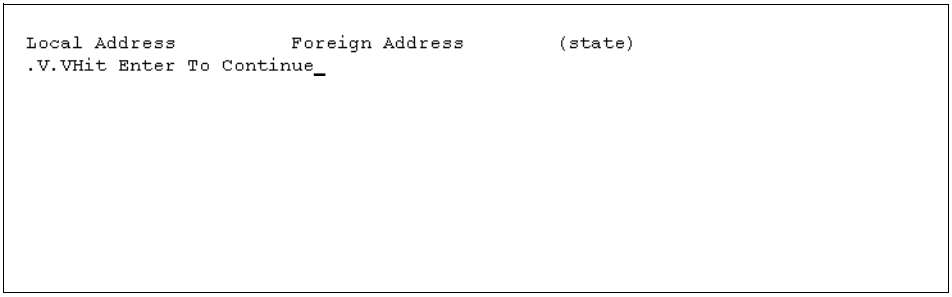


Figure 8.5 - TCP View Display

CHAPTER 9 MPOA Management

This chapter provides an overview of Multiple Protocol over ATM (MPOA) and details the menus used to manage MPOA on the ES-3810. These menus are available by selecting the Manage MPOA option from the ES-3810 Main Menu.

9.1 MPOA Overview

MPOA integrates LAN Emulation (LANE) and Next Hop Resolution Protocol (NHRP) to preserve the benefits of LANE, while allowing inter-subnet, internetwork layer protocol communication over ATM VCCs without requiring routers in the data path. MPOA provides a framework for effectively synthesizing bridging and routing with ATM in a diverse environment, providing a unified paradigm for overlaying internetwork layer protocols on ATM. Using both routing and bridging information, MPOA is capable of locating the optimal exit from the ATM cloud.

By employing virtual routing— the physical separation of internetwork layer route calculation and forwarding— MPOA provides a number of key benefits:

- Efficient inter-subnet communication;
- Increased manageability through the reduction of the number of devices that must be configured to perform internetwork layer route calculation;
- Increased scalability through the reduction of the number of devices participating in internetwork layer route calculations.

Through the use of virtual routing, MPOA reduces the complexity of edge devices, such as the ES-3810, by eliminating the need for these devices to perform internetwork layer route calculations.

The primary goal of MPOA is the efficient transfer of unicast data. To accomplish speed and efficiency of data transfer, MPOA utilizes the strengths of ATM network topology and configuration to effectively link up shortcuts between a source and destination. MPOA components establish shortcut VCCs between each other as necessary to transfer data and control messages over an ATM network.

9.1.1 MPOA Shortcuts

A shortcut is a direct one-hop path to a destination or to the nearest transit point to a destination. For a shortcut to be established: an ingress (destined toward the ATM cloud) MPC must first have been configured on the originating device; all routers connecting the originating device to the terminating device must have been configured with MPSes; and the terminating device must a have an MPC or MPS configured.

Default forwarding for the MPOA System occurs via routers. When an MPC becomes aware of a particular traffic flow that could benefit from a shortcut, the ingress MPC needs to determine the ATM address associated with the egress device (outside of the ATM cloud). To obtain the ATM address for a shortcut, the ingress MPC sends an MPOA Resolution Request to the appropriate ingress MPS. When this MPS is able to resolve the resolution request, a reply is returned to the ingress MPC that contains an ATM address of the egress device.

If a shortcut is established, the ingress MPC strips the DLL encapsulation from the packet and sends it via the shortcut. When the packet arrives via shortcut at the egress MPC, it is examined and either a matching egress cache entry is found or the packet is dropped. All encapsulated information is stored at the egress MPC/MPS and is inserted at the egress point before being passed on to legacy ports.

9.1.2 MPOA Components

MPOA is designed with a client/server architecture. There are two types of MPOA logical components: MPOA Clients (MPC) and MPOA Server(s) (MPS). An MPC can service one or more LECs and communicates with one or more MPSes. An MPS converts between MPOA requests and replies and NHRP requests and replies on behalf of the MPCs.

In its ingress role, an MPC detects flows of packets that are being forwarded over an ELAN to a router that contains an MPS. When it recognizes a flow that could benefit from a shortcut that bypasses the routed path, it uses an NHRP-based query-response protocol to request the information required to establish a shortcut to the destination. If a shortcut is available, the MPC caches the information in its egress cache, sets up a shortcut VCC, and forwards frames for the destination over the shortcut.

In its egress role the MPC receives internetwork data frames from other MPCs to be forwarded to its local interfaces/users. For frames received over a shortcut, the MPC adds the appropriate DLL encapsulation and forwards them to the higher layers (e.g., a bridge port or an internal host stack). The DLL encapsulation information is provided to the MPC by an egress MPS and stored in the MPC's egress cache.

An MPS is the logical component of a router that provides internetwork layer forwarding information to MPCs. A full NHS, as defined in NHRP, is included in the MPS. The MPS interacts with the local NHS to answer MPOA queries from ingress MPCs and provide encapsulation information to egress MPCs.

9.1.3 MPOA Information Flows

The MPOA solution involves a number of information flows that can be categorized as MPOA control flows and MPOA data flows. By default, all control and data flows are carried over ATM VCCs using LLC/SNAP (RFC 1483) encapsulation. Configuration flows use the formats described in LANE; MPSs and MPCs communicate with the LAN Emulation Configuration Server (LECS) to retrieve configuration information.

MPC-MPS control flows are used for MPC cache management. The MPOA Resolution Request/Reply allows the ingress MPC to obtain shortcut information. The ingress MPS may trigger the ingress MPC to make a request by sending the MPOA Trigger Message. The MPOA Cache Imposition Request/Reply allows the egress MPS to give the egress MPC egress cache information. Finally, either the egress MPC or an MPS may send a Purge message if it discovers that cached information has become invalid.

MPS-MPS control flows are handled by standard internetwork layer routing protocols and NHRP. MPOA does not define any new MPS-MPS protocols. MPOA requires no new replication techniques and relies upon the standard techniques provided by LANE and internetwork layer routing protocols.

MPC-MPC control flows are used to invalidate erroneous cache information. An egress MPC may send a data plane purge to an ingress MPC if it receives misdirected packets from that MPC. This causes the MPC to invalidate its erroneous cache information.

MPC-MPC data flows are used primarily for the transfer of data between MPCs over MPOA shortcut VCCs.

MPC-NHC data flows are used to allow an MPC to send unicast data to an NHC and to allow an NHC to send unicast data to an MPC.

9.1.4 MPOA Operations

MPOA performs the following operations: configuration, discovery, target resolution, connection management, and data transfer. These operations are described in the following subsections.

9.1.4.1 Configuration

MPCs and MPSes require configuration. By default, MPOA components retrieve their configuration parameters from the LECs.

MPOA components must be able to configure via the LECs.

9.1.4.2 Discovery

To reduce operational complexity, MPOA components automatically discover each other (i.e., the MPC's and MPSs "learn" of each other's existence) using extensions to the LANE LE_ARP protocol that carry the MPOA device type (MPC or MPS) and ATM address. This information is discovered dynamically and used as needed.

MPCs are not NHCs and do not register host internetwork layer addresses with NHSes using NHRP Registration.

9.1.4.3 Target Resolution

MPOA target resolution uses an extended NHRP Resolution Request protocol to allow MPCs to determine the ATM address for the end points of a shortcut. The protocol is interpreted from different perspectives by the ingress MPC, the ingress MPS, the egress MPS and the egress MPC.

An ingress MPC learns the MAC addresses of MPSes attached to its ELAN from the device type TLVs in LE_ARP responses. The MPC is required to perform flow detection, based on internetwork layer destination addresses, on packets destined for these learned MAC addresses. Additionally, an MPC is permitted to perform other types of flow detection.

The ingress MPS processes MPOA Resolution Requests sent by local MPCs. The ingress MPS can answer the request if the destination is local; otherwise, it re-originates the request along the routed path through its local NHS. To insure that the reply is returned to the originating MPS, the ingress MPS uses its internetwork layer address as the source protocol address in the re-originated request. All other fields from the MPOA resolution request are copied, in particular the MPC's data ATM address, which is used as the NBMA address, and all TLVs.

NOTE

A new Request ID is set by the ingress MPS for the re-originated request so that downstream NHSes do not cache the association of the resulting internetwork layer and ATM addresses. On receiving a reply, the ingress MPS restores the Request ID field and source protocol address and returns an MPOA Resolution Reply to the ingress MPC.

The egress MPS sources an MPOA Cache Imposition Request when an NHRP Resolution Request targeted for a local MPC arrives at the egress MPS serving that MPC. After receiving the MPOA Cache Imposition Reply from the egress MPC, the egress MPS sends an NHRP Resolution Reply toward the request originator. Additional information requested by the ingress MPC (and included in the MPOA Cache Imposition Request and the MPOA Cache Imposition Reply messages) must be included in the NHRP resolution as well.

The egress MPC must send an MPOA cache Imposition Reply for every MPOA Cache Imposition Request. To formulate its reply, the MPC must determine if it has the resources to maintain the cache entry and potentially receive a new VCC. If the MPC cannot accept either the cache entry or the VCC that might result from a positive reply, it sets the appropriate error status and returns the MPOA Cache Imposition Reply to the MPS. If the MPC can accept this cache entry, it inserts an ATM address and may modify the MPOA Egress Cache Tag Extension (if present) to be used by the ingress MPC in connection with this shortcut, sets a success status, and sends the MPOA Cache Imposition Reply to the egress MPS.

In some configurations, it is possible for an egress MPC to receive conflicting next-hop forwarding instructions for the same source ATM address and internetwork layer address pair. If this conflict occurs, the egress MPC will take one of the following actions to ensure that packets are forwarded properly: an appropriate tag in the MPOA cache Imposition Reply may be included; a distinct destination ATM address may be included in the MPOA Cache Imposition Reply; or, the imposition request may be refused.

9.1.4.4 Connection Management

MPOA components establish VCCs between each other as necessary to transfer data and control messages over an ATM network. For the purpose of establishing control VCCs, MPOA components learn of each other's existence through the discovery process described above. For the purpose of establishing data VCCs, MPOA components learn of each other's existence through the resolution process described above.

9.1.4.5 Data Transfer

The primary goal of MPOA is the efficient transfer of unicast data. Unicast data flow through the MPOA system has two primary modes of operation: the default flow and the shortcut flow. The default flow follows the routed path over the ATM network. In the default case, the ES-3810 acts as a Layer 2 bridge. Shortcuts are established by using the MPOA target resolution and cache management mechanism.

When an MPC has an internetwork protocol packet to send for which it has a shortcut, the ES-3810 acts as an internetwork level forwarder and sends the packet over the shortcut.

9.2 Manage MPOA Menu

The Manage MPOA Menu (see Figure 9.1) is reached from the Main Menu of the ES-3810 console interface by selecting the Manage MPOA option.

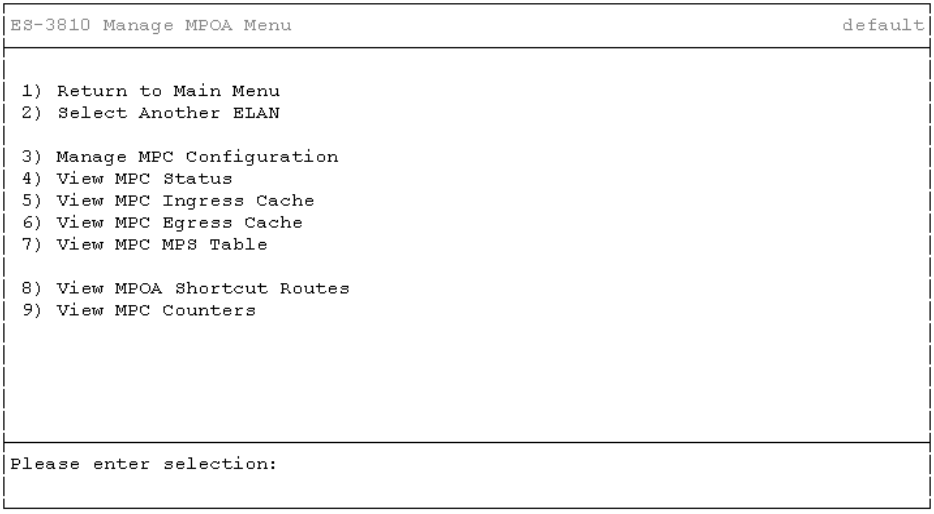


Figure 9.1 - Manage MPOA Menu

Return to Main Menu	Returns to the Main Menu.
Select Another ELAN	Returns to the ELAN Selection Menu.
Manage MPC Configuration	Displays the Manage MPC Menu.
View MPC Status	Displays the MPC Status view.
View MPC Ingress Cache	Displays the MPC Ingress Cache view.
View MPC Egress Cache	Displays the MPC Egress Cache view.
View MPC MPS Table	Displays the MPC MPS Table view.
View MPOA Shortcut Routes	Displays the MPOA Shortcut Routes view.
View MPC counters	Displays the MPC Counters view.

9.2.1 Manage MPC Configuration Menu

To view the Manage MPC Configuration Menu (see Figure 9.2), select the Manage MPC Configuration option from the Manage MPOA Menu (see Figure 9.1).

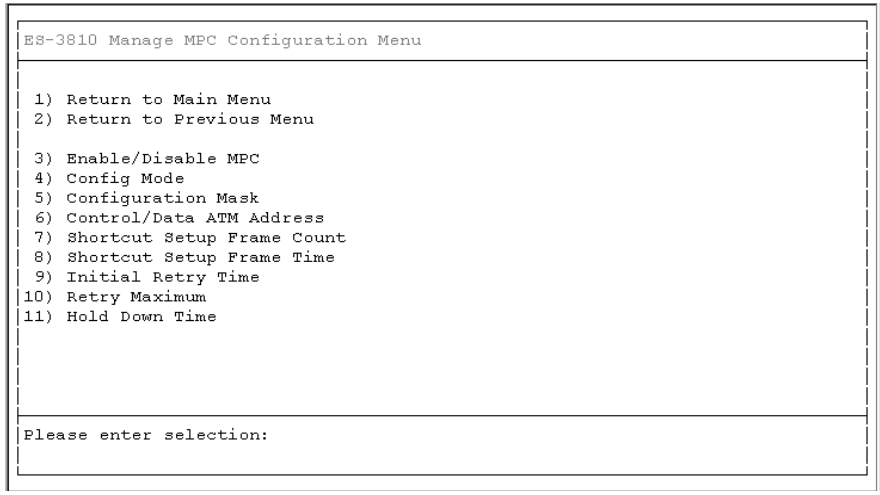


Figure 9.2 - Manage MPC Configuration Menu

Return to Main Menu	Returns you to the Main Menu.
Return to Previous Menu	Returns you to the Manage MPOA.
Enable/ Disable MPC	In this menu you can change the state of the MPC. When an MPC changes states it rejoins the ELAN.
Config Mode	In this menu you can change the state of the MPC from manual to automatic.
Configuration Mask	This menu is for debugging purposes.
Control/ Data ATM address	This menu allows you to change the control ATM address (used for MPOA control information) and the data ATM address (used to set up shortcut VCs).
Shortcut Setup Frame Count	This menu allows you to modify shortcuts and frame counts.
Shortcut Setup Frame Time	This menu allows you to modify shortcuts and frame time.

NOTE

The MPC will initiate a shortcut when it sees the numbers specified in the shortcut frame time and count. For instance, if the frame count is set at 10 and the time is set at 1-second, the MPC will initiate a shortcut when it sees 10 frames in 1-second.

Initial Retry Time When the MPC does not receive a shortcut resolution response, then it will wait for this initial retry time before trying the resolution again.

Retry Maximum Each time the MPC fails to get a response, it will wait for a longer time. This the limit on that amount of time.

Hold Down Time The minimum amount of time to wait before re-initiating a failed resolution attempt.

9.2.1.1 Enabling and Disabling MPC

This screen is reached from the Manage MPC Menu (see Figure 9.2); in it you will be prompted to switch states of the MPC, so that it is either enabled or disabled.

NOTE

When an MPC changes states it rejoins the ELAN.

9.2.1.2 Configuration Mode

This screen is reached from the Manage MPC Menu (see Figure 9.2); in it you will be prompted to switch states of the MPC from manual to automatic.

NOTE

When an MPC changes states it rejoins the ELAN.

NOTE

If the configuration mode is automatic, all of the MPOA parameters are taken from LECs. In manual mode, parameters are locally assigned defaults. You can change these in the MPC Configuration Menu.

9.2.1.3 Enabling/Disabling MPCs on an ELAN

To reach the Enable / Disable view (see Figure 9.3) select the Enable / Disable MPC option from the Manage MPC Configuration Menu (see Figure 9.2). In this screen you are allowed to enable or disable MPC on an ELAN.

```
The current ELAN's mpc is Disabled.

Do you want to change it to Enabled? [No]?  y
Enter MPC Configuration Mode: 1=Auto; 2=Manual [1]?1
Enabling MPOA Client 0
Enabling MPOA Client 16

Hit <Enter> to continue.
```

Figure 9.3 - MPC Enable / Disable View

9.2.1.4 Shortcut Setup Frame Count

To reach the Shortcut Setup Frame Count view (see Figure 9.4) select the Shortcut Setup Frame Count option from the Manage MPC Menu (see Figure 9.2). This menu allows you to modify shortcut frame time.

The MPC will initiate a shortcut based on the numbers specified in the shortcut frame time and count. For instance, if the frame count is set at 10 and the time is set at 1-second, the MPC will initiate a shortcut when 10 frames in 1-second are specified.

```
The current shortcut setup Frame Count is 10.

Enter the new Frame Count[1 - 65535]: _
```

Figure 9.4 - Shortcut Frame Count

9.2.1.5 Shortcut Setup Frame Time

To reach the Shortcut Setup Frame Time view (see Figure 9.5) select the Shortcut Setup Frame Time option from the Manage MPC Menu (see Figure 9.2). This screen allows you to modify shortcuts and frame count.

The MPC will initiate a shortcut when it sees the numbers specified in the shortcut frame time and count. For instance, if the frame count is set at 10 and the time is set at 1-second, the MPC will initiate a shortcut when it sees 10 frames in 1-second.

```
The current shortcut setup Frame Time is 1.

Enter the new Frame Time[1 - 60]: _
```

Figure 9.5 - Shortcut Frame Time

9.2.1.6 Initial Retry Time

To reach the Initial Retry Time view (see Figure 9.6) select the Initial Retry option from the Manage MPC Configuration menu (see Figure 9.2). In this screen you are allowed to change the initial retry time.

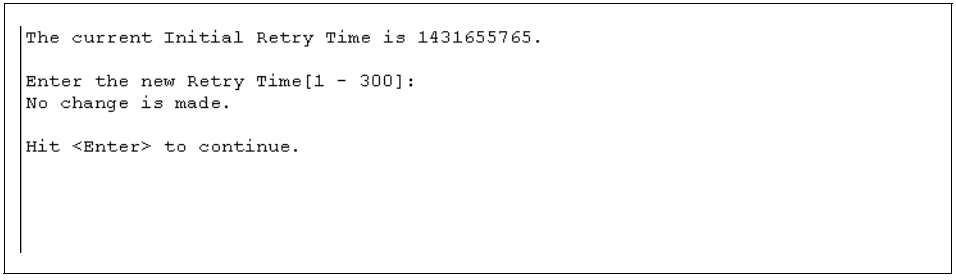


Figure 9.6 - Initial Retry Time

Initial Retry Time When the MPC does not receive a shortcut resolution response, then it will wait for this initial retry time before trying the resolution again.

9.2.1.7 Retry Maximum

To reach the Retry Maximum view (see Figure 9.7) select Retry Maximum from the Manage MPC Configuration menu (see Figure 9.2). This screen allows you to change the maximum amount of time that the MPC will wait before trying to get a response after the initial attempt has failed.

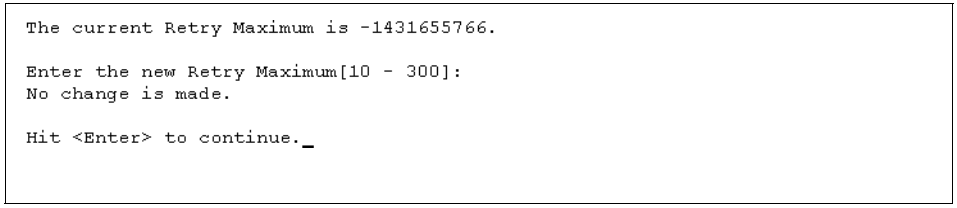


Figure 9.7 - Retry Maximum

Retry Maximum The limit on the amount of time that the MPC will wait to get a shortcut resolution response.

NOTE Each time the MPC fails to get a response, it will wait for a longer time, unless Retry Maximum is set to limit that amount of time.

9.2.1.8 Hold Down Time

To reach the Hold Down Time view (see Figure 9.8) select the Hold Down Time option from the Manage MPC Configuration menu (see Figure 9.2). This screen allows you to change the preset hold down time.

```
The current Hold Down Time is 1431655765.

Enter the new Hold Down Time[30 - 1200]: 40

Hit <Enter> to continue.
```

Figure 9.8 - Hold Down Time

Hold Down Time The minimum amount of time the MPC will wait before re-initiating a failed shortcut resolution attempt.

9.2.2 MPC Status

To reach the MPC Status View (see Figure 9.9) select View MPC Status from the Manage MPOA menu (see Figure 9.1). This screen allows you to switch the state of the MPC status from `Disabled` to `In Service`.

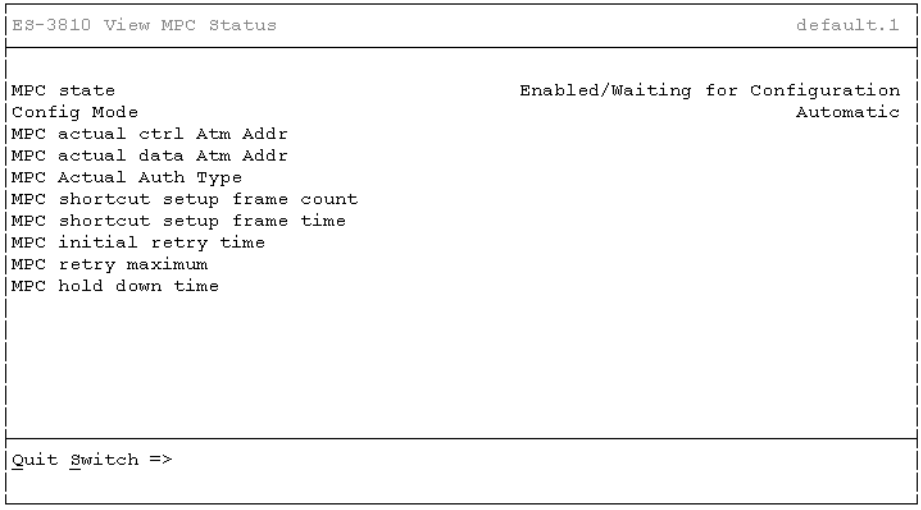


Figure 9.9 - MPC Status View

MPC State	Displays the operational status of the MPC, which is either in service, waiting for configuration information, or disabled.
Config Mode	This mode is either manual or automatic.
MPC Actual Control ATM Address	Displays the address of the control ATM (used for MPOA control information) and the data ATM address (used to set up shortcut VCs)
MPC Actual Data ATM Address	Displays the address of the data ATM address (used to set up shortcut VCs).
MPC Actual Auth Type	Displays the authentication type.
MPC Shortcut Setup Frame Count	Displays shortcut setup frame count.
MPC Shortcut Setup Frame Time	Displays shortcut setup frame time.
MPC Initial Retry Time	When the MPC does not receive a shortcut resolution response, then it will wait for this initial retry time before trying the resolution again.
MPC Retry Maximum	Displays the limit on the amount of time that the MPC will wait to get a shortcut resolution response.
MPC Hold Down Time	Displays the minimum amount of time the MPC will wait before re-initiating a failed shortcut resolution attempt.

9.2.3 MPC Ingress and Egress Caches

To reach the MPC Ingress Cache View (see Figure 9.10) and the MPC Egress Cache View (see Figure 9.11) select the View MPC Ingress Cache option or the View MPC Egress Cache option, respectively, from the Manage MPOA menu (see Figure 9.1). These screens allow you to view the MPC Ingress and Egress Caches.

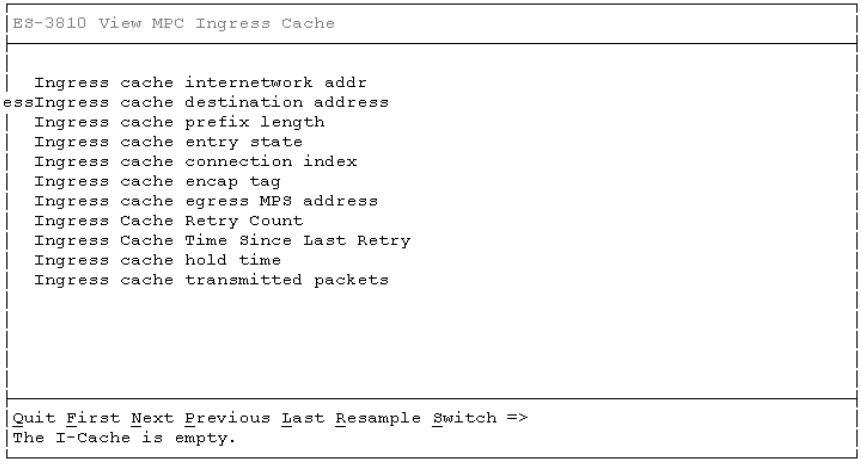


Figure 9.10 - MPC Ingress Cache View

Ingress:	Information travelling from the ES-3810 towards ATM.
Internetwork Address	Displays the IP address.
Prefix Length	Displays the network portion of the IP address.
Entry State	Displays a state which can be either resolved, unresolved, or invalid. For instance, if a shortcut is set up for this destination, then the state is resolved.
Connection Index	Displays information used for debugging.
Encap Tag	Displays a cache tag for the Egress MPC, to be used for sending packets over the shortcut.
Retry Count	Displays the number of times resolution was attempted.
Time Since Last Retry	Displays the time elapsed since the last failed resolution attempted.
Hold Time	Displays the amount of time that Ingress cache entry will remain valid.
Transmitted Packets	Displays the number of transmitted packets.

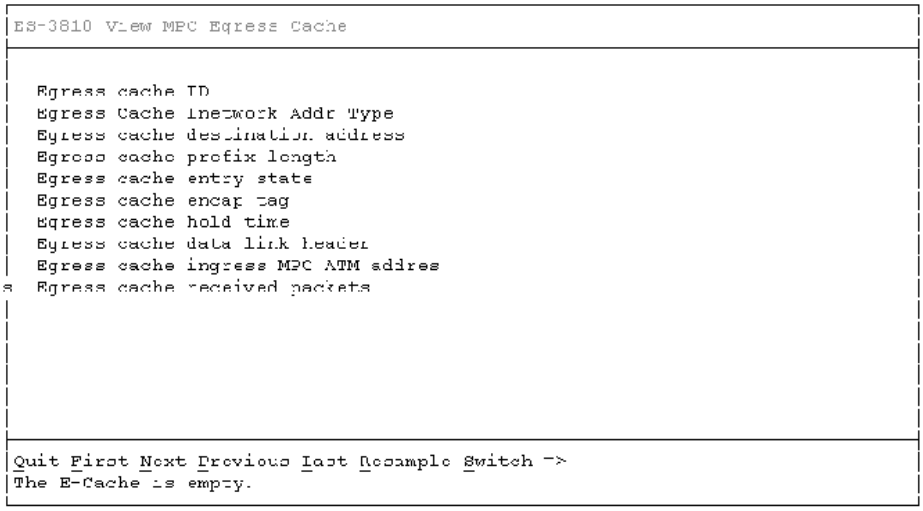


Figure 9.11 - MPC Egress Cache View

Egress: Information travelling from ATM into the ES-3810.

Cache ID Displays an identifier sent from Egress MPS to MPC.

Destination Address Displays the destination IP address of the traffic.

Entry State Displays either a resolved or unresolved entry state.

Encap Tag Displays the cache tag for the Ingress MPC to be used for sending packets over the shortcut.

Hold Time Displays the amount of time that Egress cache entry will remain valid.

Data Link Header Displays the DLL encapsulation that is used to forward packets.

Received Packets Displays the number of packets received.

9.2.4 MPC MPS Table

To reach the MPC MPS Table (see Figure 9.12) select the View MPC MPS Table from the Manage MPOA menu. This screen allows you to view ATM and MAC addresses.

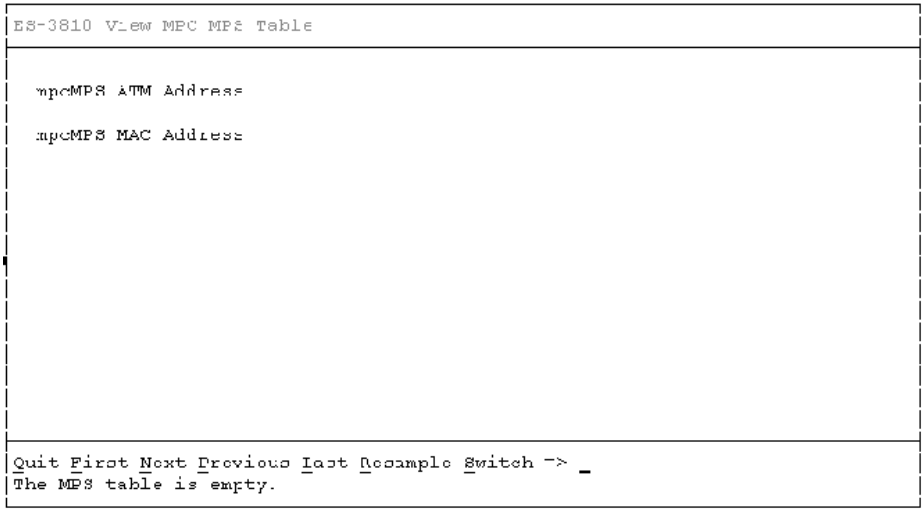


Figure 9.12 - MPC MPS Table View

mpcMPS ATM Address	Displays the ATM address of the MPS that was detected by the MPC.
mpcMPS MAC Address	Displays the MAC address of the MPS.

9.2.5 MPOA Shortcut Routes

To view the MPOA Shortcut Routes view (see Figure 9.13) select the View MPC Shortcut Routes from the Manage MPOA menu (see Figure 9.1). This screen displays the shortcut routes.

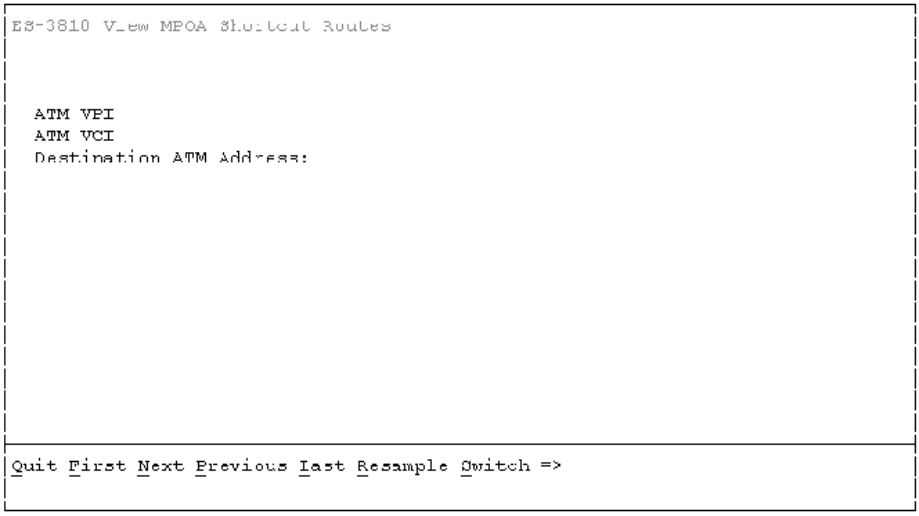


Figure 9.13 - MPOA Shortcut Routes View

9.2.6 MPC Counter

To reach the MPC Counter view (see Figure 9.14) select the View MPC Counters option from the Manage MPOA menu (see Figure 9.1).

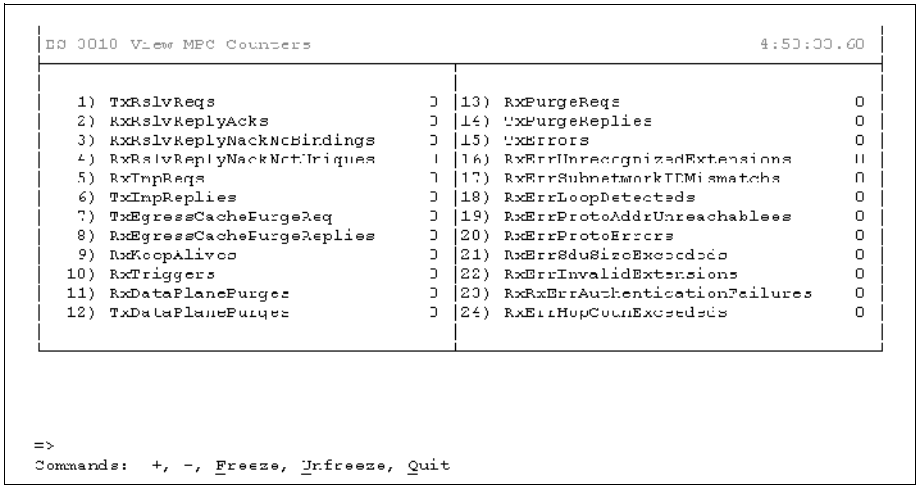


Figure 9.14 - MPC Counter View

APPENDIX A ESM-16 Console Management Subsystem

The following details the menu selections available through the ESM-16 Console Management Subsystem. The ESM-16 Console Management Subsystem is not used in systems with an NMM or an NMC. If your system is configured with a either of these modules, please ignore this chapter and refer to Chapters 1 through 8.

The following sections detail the menu selections available through the ESM-16 Console Management Subsystem.

A.1 The Main Menu

The following is the main menu that will be displayed. This is the first menu displayed upon power up, as well as the menu that remains displayed after any menu selection is completed.

ForeRunner ES-3810
Copyright 1995 FORE Systems, Inc.
Main Menu

1. View Port Configuration
2. View Port Counters
3. Set Port Configuration
4. Address Database Functions
5. Save Current Settings
6. Reset to Factory Default Settings
7. Download New Image
8. Initialize Port Counters
9. Reboot

Enter Selection:

A.1.1 View Port Configuration

The following menu is displayed for option 1 from the Main Menu.

The user will first be prompted for a port number to view.

ForeRunner ES-3810
Port Configuration

Please enter port number (1-16): 1
Firmware Version: V1.1.00
Hardware Version: 10B

Port implementation:	**SEC-10**	**Transmitter:**	**ENABLED**
Chip number:	**0**	**Receive Buffer:**	**ENABLED**
Twisted Pair:	**ENABLED**	**Transmit Buffer:**	**ENABLED**
Loopback:	**DISABLED**	**Secure Learn:**	**DISABLED**
Sniff Segment:	**DISABLED**	**Receive Err Pkts:**	**DISABLED**
Full Duplex:	**DISABLED**	**Hash Uploading:**	**DISABLED**
Force Transmit:	**DISABLED**	**Flagged Packets:**	**DISABLED**
Polarity Correction:	**DISABLED**	**Sniffed Packets:**	**DISABLED**
Link Detected:	**NO**	**IA Promiscuous:**	**DISABLED**
Link Polarity:	**OK**	**MC Promiscuous:**	**ENABLED**
Receiver:	**ENABLED**	**Backbone Mode:**	**DISABLED**

Press ENTER to Return to Main Menu

A.1.2 View Port Counters

The following menu is displayed for Option 2 from the Main Menu.

NOTE

The user will first be prompted for a port number to view.


```
                    ForeRunner ES-3810
                    View Port Statistics

Please enter port number (1-16): 1

--------- TRANSMITTER ----------      ---------- RECEIVER ----------
Total Bytes:              1202010372   Total Bytes:              335294917
Packets:                  2832049      Packets:                  2293755
Lost Packets:             0            Lost Packets:             0
Broadcasts:               30862        Broadcasts:               69083
Multicasts:               175576       Multicasts:               69083
Single Collisions:        2299         Short Packets             0
Multiple Collisions:      2439         Long Packets:             0
Excessive Collisions:     0            Framing Errors:           0
NCL Packets:              0            FCS Error Packets:        0
Init Deferred Pkts:       113645       Late Collisions:          0


  Press ENTER to Return to Main Menu
```

A.1.3 Set Port Configuration

The following menu is displayed for Option 3 from the Main Menu.

The user will first be prompted for a port number for which the parameters will be set. It is recommended that before any parameter is set to anything other than the Factory Default Setting, a thorough understanding of Section 8.2.1, Port Parameters, is required.

ForeRunner ES-3810
Set Port Attributes

The following attributes are settable:

1. Enable/Disable Loopback Mode	**2. Enable/Disable Segment Sniffing**
3. Enable/Disable Full Duplex Mode	**4. Enable/Disable Receiver**
5. Enable/Disable Transmitter	**6. Enable/Disable Secure Learning**
7. Enable/Disable Hash Upload	**8. Enable/Disable Flagged Packets**
9. Enable/Disable Packet Sniffing	**10. Enable/Disable IA Promiscuous Mode**
11. Enable/Disable MC Promiscuous Mode	**12. Enable/Disable Backbone Mode**
13. Enable/Disable Receive Errors Mode	**14. Enable/Disable Twisted Pair Mode**
15. Enable/Disable Correct Polarity	**16. Enable/Disable Force Tmit Mode**
17. Enable/Disable Rx Ring Buffer	**18. Enable/Disable Tx Ring Buffer**

Please Enter Selection [range 1-18]:

For each of the parameters that may be set, the current state of the parameter is presented and the user is asked a final time if they are sure they want to change the parameter.

CAUTION

Any changes made are immediately implemented. Make sure you read Section 8.2.1 and have a thorough understanding of the port parameters.

A.1.4 Address Database Functions

Each port of the ES-3810 maintains an address database for the four addresses maintained for that port. These parameters can be either viewed or modified. Once the Address Database Functions option has been selected, a submenu is presented with three options - Option 1 allows the address aging time to be set, Option 2 allows address database viewing and Option 3 allows address database modifications.

```
ForeRunner ES-3810
Address Database Functions

1. Set Address Aging Time
2. View Address Database
3. Modify Address Database

Enter Selection:
```


A.1.4.1 Set Address Aging Time

By default, the ES-3810 will not automatically age idle addresses, that is, once learned, an address will stay within the respective ports address database until either a switch reboot or new addresses are learned by the port. The Set Address Aging Time option allows the network administrator to set a time limit on how long an idle address will reside within a ports address database before the firmware will age the address.

```
ForeRunner ES-3810
Set Address Aging Time

Please enter the Address Aging Time <0 - 59>: 20
Press ENTER to Return to Main Menu
```

The time entered is a global parameter. In the preceding example all addresses within all ports of the ES-3810 will age in 20 minutes if they are idle for that length of time.

A.1.4.2 View Address Database

The View Address Database option lets the contents of a port's address database to be displayed.

```
                    ForeRunner ES-3810
                Address Database Functions

                                        Age     Multicast
Address             Flagged             Flag    Mask        Hash

00-A0-36-00-01-02   No                  0       FFFF        No
00-A0-36-00-03-04   Yes                 3       FFFF        No
00-A0-36-00-05-06   Yes                 1       4           No
00-A0-36-00-07-08   No                  2       B           No

Press ENTER to Return to Main Menu
```

A.1.4.3 Modify Address Database

The Modify Address Database Options allows for the modification of all the address database parameters.

```
                    ForeRunner ES-3810
                Modify Address Database


Address 1:      00-A0-36-00-01-02       Age:    3
Address 2:      00-A0-36-00-03-04       Age:    0
Address 3:      00-A0-36-00-05-06       Age:    1
Address 4:      00-A0-36-00-07-08       Age:    2

The following parameters may be set within the address database:
        1. Age Information (0, 4, 5, or 7)
        2. An Individual Address (form aabbccddeeff)
        3. Multicast Domain (0h - Fh)
        4. Enable/Disable Flag Bit
Please Enter Selection: 1
Please Enter Address From Above (1-4): 1
Enter New Age Information: 5

Press ENTER to Return to Main Menu
```

A.1.5 Save Current Settings

The Save Current Settings option allows for any port parameter customization that has been performed to be saved in non-volatile storage. In this way, these parameter customizations are automatically restored upon an ES-3810 reboot or power cycle.

ForeRunner ES-3810
Save Current Settings

Saving Port Parameters .....
Press ENTER to Return to Main Menu

A.1.6 Reset to Factory Default Settings

The Reset to Factory Default option causes a full reset for each port of the ES-3810, resetting each ports entire parameter configuration to the default settings detailed in Section 3.4.1. When this option is selected, any customized settings that have been saved in non-volatile storage are cleared.

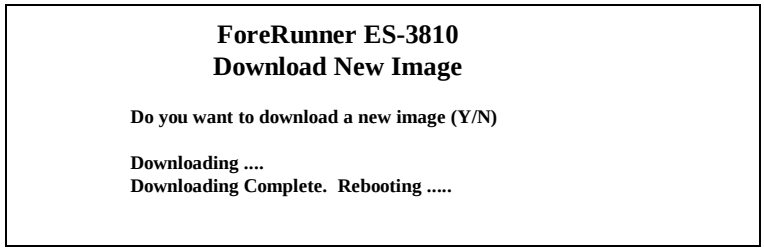
ForeRunner ES-3810
Reset to Factory Defaults

Resetting Port parameters .....
Press ENTER to Return to Main Menu

A.1.7 Download New Image

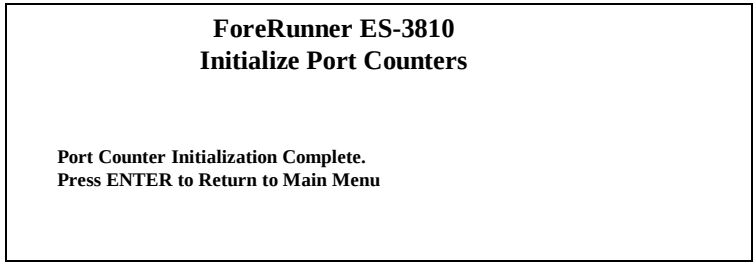
The Download New Image option allows for firmware upgrades to be made to the *ForeRunner* ES-3810. The download option is built upon the XMODEM protocol; therefore, the management station must support the XMODEM protocol and must have the ability to load a software image onto a media device (e.g., hard disk, diskette).

The Download New Image option is a two-stage process - first, the option must be selected and second, the XMODEM protocol must be initiated. Once the option is selected, choose the binary transfer option from the XMODEM based application on the management station (e.g., Microsoft Windows 3.x Terminal). When prompted, enter the path where the file ES3810cm.BIN has been placed. The download takes approximately one minute to complete. Once the download finishes, the ES-3810 performs an automatic reboot.



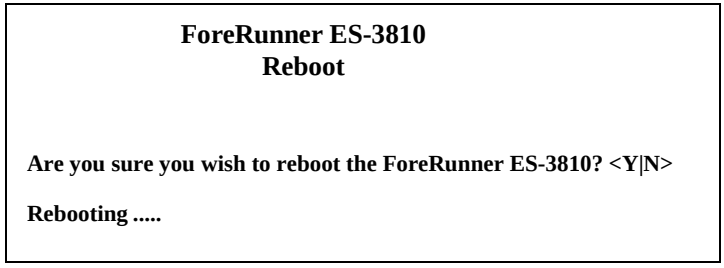
A.1.8 Initialize Port Counters

The Initialize Port Counters option resets, on a port-by-port basis, the counters displayed (see Section 8.1.2) to all zeros.



A.1.9 Reboot

The Reboot option performs a full initialization of the ES-3810. The power-up sequence detailed in Section 1.3 takes place.



A.2 Port Characteristics

A.2.1 Port Parameters

The following section provides a brief description of each of the port's characteristics.

TwistedPairMode When enabled, the port configures its transceivers as a standard twisted pair device. When disabled, the port configures the transceiver as an asynchronous NRZ interface designed to interface directly to a serial interface adapter.

LoopbackMode When enabled, data sent by the transmitter is looped back to the receiver and all data from the receiver and collision input pins is ignored. When disabled, the port acts as a standard Ethernet CSMA/CD port.

The Loopback Mode is intended for diagnostic purposes only and should remain disabled.

SniffSegmentMode When disabled, the port acts as a normal CSMA/CD port. When enabled, all packets sent by the transmitter are looped back to the receiver, but the receive and collision logic is not disabled. SniffSegmentMode forces all packets on a half-duplex port (sent and received) through the receiver to the Packet Bus allowing the segment to be "sniffed" elsewhere in the ES-3810.

FullDuplexMode When disabled, each port acts as a 10 Mbit/sec CSMA/CD port. When enabled, the port acts as a 20 Mbit/sec port. Full Duplex mode indicates that send and receive can happen simultaneously.

ForceTransmissionMode When disabled, the port acts as a standard 10 Mbit/sec CSMA/CD port. When enabled, packets are transmitted regardless of the state of the transceiver.

This parameter is for diagnostic purposes only and should remain disabled at all times.

CorrectPolarity Mode — When enabled, data polarity can be corrected when the receiver is in an incorrect polarity mode. When disabled, data polarity correction logic is disabled.

LinkFailMode — This informational parameter indicates the status of the link integrity state. When OK, the port is operating properly; when Wrong, the link detection circuitry detected an error.

WrongPolarity Mode — This informational parameter indicates the status of the polarity logic. When disabled, the received polarity of the packet is good. When enabled, the polarity is incorrect.

ReceiverMode — When enabled, the receiver portion of the Media Access Controller ("MAC") is active. When disabled, the receiver portion of the MAC is inactive.

ReceiveRingBufferMode — When enabled, the memory ring buffer used for packet reception is active. When disabled, the receive ring buffer becomes inactive.

ReceiverMode and ReceiveRing BufferMode must be enabled to receive packets on the port.

TransmitterMode — When enabled, the transmitter portion of the Media Access Controller ("MAC") is active. When disabled, the transmitter portion of the MAC is inactive.

TransmitterRing BufferMode — When enabled, the memory ring buffer used for packet transmission is active. When disabled, the transmit ring buffer becomes inactive.

TransmitterMode and TransmitterRingBufferMode must be enabled to transmit packets on the port.

SecureLearnMode — When disabled, newly learned addresses are automatically used for forwarding from the Packet Bus to the Ethernet. When enabled, new addresses are stored in the address database but are only used for forwarding after the management processor confirms the validity of the newly learned address.

NOTE This feature is only available for in-band management configurations.

ReceiveErrorsMode When enabled, all packets, including those with errors, are forwarded onto the Packet Bus. When disabled, received packets with errors are automatically deleted from the receive ring buffer memory and, therefore, are not forwarded on to the Packet Bus.

UploadMode This parameter is reserved for future use.

FlaggedPacket Mode When enabled, and none of the individual address flag bits are set, all packets with the flag bit set will be received from the Packet Bus and transmitted by the port. When enabled, and any of the individual address bits are set, packets with the flag bit set are received from the Packet Bus if the destination address matches one of the flagged addresses in the port's address database. When disabled, flagged packets are treated like any other packet on the Packet Bus.

SniffedPacket Mode When enabled, all sniffed packets (transmitted or received) are taken from the Packet Bus and transmitted on the port. When disabled, sniffed transmit packets are ignored by this port and sniffed receive packets are handled like any other packet on the Packet Bus.

IndividualAddressPromiscuous Mode When enabled, all individually addressed packets from the Packet Bus are transmitted by the port. When disabled, normal filtering is performed on individually addressed packets from the Packet Bus, such as matching the destination address with the addresses in the ports address database.

MulticastAddress PromiscuousMode When enabled, all multicast messages from the Packet Bus are transmitted by the port. When disabled, normal filtering is performed on multicast messages from the Packet Bus.

BackboneMode When enabled, the port transmits all individually addressed packets whose destination address does not reside in any of the ports' address databases.

When disabled, or in Workgroup Mode, normal operation is selected and only those individual addresses that match an entry in the ports' address database are received from the Packet Bus.

If all ports are in Workgroup Mode and a packet match does not occur within any port, the packet is simply dropped.

A.2.2 Address Databases

Each Workgroup port of an ES-3810 maintains a four-entry address database that is maintained in a dynamic fashion (i.e., addresses are learned, aged, and migrated in a dynamic, interactive nature). Additionally, each address database entry maintains certain characteristics about the address as follows:

Age Information — Each of the four addresses are numbered zero (0) through three (3) with zero being the most recently learned address and three being the oldest address in the database. Further, if an address was learned in SecureLearnMode, the age field is four (4) and the address is used for forwarding only after the management processor locks the address (which turns the age field to five (5) or acknowledges it (age=zero (0)). If an address has an age value of five (5), it will not be aged or migrated.

Hash Information — A one (1) in this field indicates a multicast hash table has been uploaded to the port from an end station.

Domain Information — This 16-bit field represents the virtual LAN, or multicast domain, information for the address. Each of the 16 bits represents a separate and unique virtual LAN/multicast domain to which this address can belong.

Index

N